Överkursmaterial i kryptografi för högstadieelever

Pro gradu-avandling, Helsingfors universitet

Studerande:
Sandra Westerlund

Handledare:
Johanna Rämö
Hans-Olav Tylli
Anne-Maria Ernvall-Hytönen

7 juni 2020

UNIVERSITY OF HELSINKI

Tiedekunta - Fakultet - Faculty	Laitos - Institution - Department	
Matematisk-naturvetenskapliga fakulteten	Institutionen för matematik och statistik	
Tekijä - Författare - Author		
Sandra Westerlund		
Työn nimi - Arbetets titel - Title		
Överkursmaterial i kryptografi för högstadieelever		
Oppiaine - Läroämne - Subject		
Matematik, ämneslärarlinjen		
Työn laji - Arbetets art - Level	Aika - Datum - Month and year	Sivumäärä - Sidoantal - Number of pages
Pro gradu-avhandling	September 2020	35 sidor. + 7 bilagor

Tiivistelmä - Referat - Abstract

Temat för den här pro gradu-avhandlingen är skapandet av ett e-läromedel för särbegåvade niondeklassister i matematik. Mycket forskning visar på att särbegåvade elever finner skolgången tråkig och att den ger för få utmaningar. Detta i sin tur leder till att en del särbegåvade elever till och med underpresterar trots deras särbegåvning. För att motverka denna trend skapades ett e-läromaterial som är riktat till särbegåvade elever. E-läromaterialet är utformat för att vara utmanande och annorlunda för att motivera de särbegåvade eleverna. Temat för e-läromaterialet är kryptografi i samband med detta tema tangeras bland annat primtal, modulär aritmetik och RSA-kryptering.

Förutom själva e-läromaterialet så behandlar avhandlingen också definitionen av särbegåvade elever och på vilka olika sätt elever kan vara särbegåvade. I samband med detta undersöks också hur lärare beaktar elevernas särbegåvning, samt lärarnas förmåga att stöda och identifiera särbegåvade elever. Denna aspekt undersöks både sett från deras möjligheter att göra så tidsmässigt, samt deras skyldighet att göra så utgående från läroplanen. I avhandlingen undersöks också definitionen e-läromaterial, samt jämförs e-läromaterialet om kryptografi med riktlinjer för goda e-läromaterial, vilka getts av Utbildningsstyrelsen. Som sammanfattning på avhandlingen förklaras de matematiska termerna och koncepten som finns i e-läromaterialet.

Avainsanat – Nyckelord - Keywords

Matematik, pedagogik, e-läromedel, särbegåvade elever

Säilytyspaikka - Förvaringsställe - Where deposited

Muita tietoja - Övriga uppgifter - Additional information

Innehåll

Inledning

I dagens skolvärld sätts det mycket resurser på stödundervisning åt elever som behöver särskilt stöd för att klara av den vanliga undervisningens svårighetsgrad. Det som dock ofta kommer i skymundan är behovet av stödundervisning för elever med särbegåvning i skolans olika ämnen. Matematikundervisningen skiljer sig inte från mängden i denna bemärkning, utan matematiskt begåvade elever får i dagens läge ofta inte det stöd som de är i behov av. Eftersom det nästan alltid är en fråga om resurser så finns det ett konstant behov av lättanvända och lättillgängliga material. Ett sätt att fylla behovet av materialen är att skapa e-läromaterial vilka kan vara öppna för alla. Detta lade grunden för skapandet av mitt eget e-läromaterial.

Syftet med min pro graduavhandling har varit att skapa ett e-läromaterial med temabaserad helhet. E-läromaterialet är riktat åt niondeklassister med särbegåvning i matematik. Temahelheten jag valde att rikta in mig på med mitt e-läromedel var kryptografi. Detta bland annat för att koppla matematiken till ett annat ämne och på så vis väcka elevernas intresse. E-läromaterialet kan tillämpas för såväl närundervsining som distansundervisning och man kan jobba med e-läromaterialet antingen i grupp eller självständigt.

Avhandlingen är uppdelad i tre delar. I den första delen presenteras begreppet särbegåvad och hur elever med särbegåvning tas i beaktande i undervisningen i dagens läge. Förutom att definiera särbegåvning tangeras även begreppet e-läromaterial och hur såväl e-läromaterial, som särbegåvning behandlas i läroplanen. Den andra delen av avhandlingen handlar om e-läromaterialet jag skapat och hur det ser ut, samt hur jag hade planerat att det skulle användas. Sista delen av avhandlingen bygger upp matematiken bakom e-läromaterialet. Medan själva e-läromaterialet är riktat åt niondeklassister, så riktar sig denna del åt lärare för att ge dem en djupare förståelse för fenomenen som undervisas åt eleverna. Som helhet så ger min avhandling en helhetsbild av hur man kan ge särbegåvade elever stöd i sin inlärning med hjälp av undervisning med temabaserat e-läromaterial.

Bevisen och strukturen i den matematisk delen av denna avhandling har fått intryck av Häsä & Rämö (2012) samt Kobliz (1994). Som största inspirationskälla för såväl bevis som struktur har jag fått från Ernvall-Hytönens (2013) kursmaterial *Elementär talteori*.

Tanken bakom e-läromaterialet

Som Pro gradu-avhandling har jag valt att skapa ett e-läromaterial för särbegåvade elever inom matematiken. Detta material är specifikt riktat till niondeklassister med särbegåvning, eftersom materialet tar upp sådana matematiska koncept som kommer att finnas på gymnasienivå. För de särbegåvade eleverna ger detta alltså en liten inblick i hur gymnasiets matematik kan se ut och förhoppningsvist fungerar det också som en motivationshöjare för dem.

Temat för materialet är kryptografi och detta har jag valt av två orsaker. Första orsaken är att matematiken bakom den kryptografi som tas upp går att förklara ganska enkelt, trots att den är något invecklad. Den andra orsaken är att kryptografi inte är ett tema som tas upp i skolorna i vanliga fall. Jag valde med avsikt ett tema som inte tas upp i skolorna vanligtvis eftersom eleverna då får lära sig något helt nytt. I detta kapitel kommer jag öppna begreppet särbegåvning, argumentera för hur ett bra e-läromedel ser ut och reflektera kring det egna materialets koppling till läroplanen.

2.1 Särbegåvning

Begreppet särbegåvning är inget lätt begrepp att vare sig förklara, eller definiera. Jag börjar med att ge en kort förklaring av de vanligaste användningssätten av ordet särbegåvning, för att sedan gå vidare till dess betydelse i olika ämnen, för att till sist gå vidare till att fundera på dess betydelse inom matematiken. Hur man urskiljer eleverna med särskild matematisk begåvning kommer jag också ge en inblick i. Sist men inte minst kommer jag också fundera på lärarnas förmåga, möjlighet och skyldighet att undervisa särbegåvade elever enligt deras egna förutsättningar.

2.1.1 Begreppet särbegåvning

För att kunna analysera begreppet särbegåvning måste vi först fundera på vad begåvning betyder. I Finland vill man inte definiera olika elever som begåvade och mindre begåvade. I vårt samhälle så vill vi snarare benämna alla elever som begåvade, vilket ger ordet litet värde. Elever som anses vara extra duktiga i ett ämne går därför under kategorin särbegåvade. Med särbegåvade elever menar man oftast elever som har en större begåvning än övriga elever i samma årskurs inom ett visst område. Speciellt det att man lär sig läsa, skriva och räkna i tidig ålder brukar vara klara tecken på särbegåvning. Detta betyder givetvist inte att det endast skulle finnas särbegåvade elever inom matematiska och akademiska ämnen.

Enligt Marland (1971) kan man kategorisera särbegåvning i sex olika grupper; intellektuell förmåga, akademisk förmåga, psykomotorisk förmåga, kreativ/produktiv förmåga,

ledarskapsförmåga och konstnärlig förmåga. Denna klassificering har dock mött motstånd från bland annat Persson (1997), som anser att denna uppdelning inte är tillräckligt breddad. Marlands uppdelning baserar sig långt på att särbegåvning går hand i hand med högt uppmätt IQ. Persson å sin sida anser att man bör klassificera särbegåvade elever enligt följande uppdelning; en idrottslig begåvning, en kommunikativ begåvning, en akademisk begåvning, en språklig begåvning, en konstnärlig begåvning och en teknisk begåvning. Persson understrycker dock att denna klassificering inte är totalt sanningsenlig, utan snarare riktlinjer som överensstämmer med samhällets intressen och värderingar. I tabellen 2.1 finns uppdelningen av Perssons kategorier, samt en kort beskrivning av dem (Eriksson, 2010).

Domängrupp	Gemensam nämnare
Idrottslig	Deras huvudsakliga aktivitet är motorisk och bygger mer eller mindre på kroppslig koordination.
Kommunikativ	Ledarskapsegenskaper; kommunicera och förmedla med kvalitativt eller kvantitativt syfte.
Akademisk	Denna domän är den som bäst sammanfaller med skolsärbegåvning, beskrivs av uppmätt IQ. Kunskapssökande, vetande och kunskapsgenererande.
Språklig	Lingvistisk intelligens; känslighet för ljud, språkrytm och semantik.
Konstnärlig	Metaperception; en inre manipulativ process som innebär ett övervakande av intryck och upplevelser. Estetiskt uttryck.
Teknisk	Hantverksmässighet, praktisk kunskap och tillämpning.

Tabell 2.1: Perssons kategorier med förklaringar

Även andra delar Perssons åsikter om särbegåvning. Bland annat Gardner (1999) delar åsikten om att särbegåvning handlar om mer än bara högt IQ. Gardner har dock valt att inte tala om särbegåvning, utan anser istället att människor har olika intelligenser. Till skillnad från Persson, som har definierat sex olika grupper med begåvningar, anser Gardner att det finns sju olika intelligenser. I tabell 2.2 finns en lista på intelligenserna listade av Armstrong (1998) med en kort sammanfattning av Petterson (2008).

Det många forskare är eniga om är att precis som elever med svårigheter i skolan behöver stöd, så är också särbegåvade elever i behov av specialundervisning och stöd för att utvecklas. Många forskningar visar att elever som är särbegåvade behöver utmaningar för att kunna utvecklas till sin fulla potential. Detta har uppmärksammats av Europarådet som också har rekommenderat att särskild undervisning bör ges åt elever med särbegåvning (Europarådet, 1994).

> *"... legislation should recognize and respect individual differences. Highly gifted children, as with other categories, need adequate educational opportunities to develop their full potential.../... the ordinary school system should be made*

Intelligens	Gemensam nämnare
Lingvistisk intelligens	Känsla för ljud, struktur, betydelse och funktion hos ord och språk.
Logisk-matematisk intelligens	Känsla för och förmåga att urskilja logiska och numeriska mönster och förmåga att resonera logiskt i långa sekvenser.
Spatial intelligens	Förmåga att uppfatta den visuella-spatiala världen korrekt och kunna omforma sina ursprungliga uttryck.
Kroppslig-kinestetisk intelligens	Förmåga att kontrollera sina kroppsrörelser och att handskas skickligt med föremål.
Musikalisk intelligens	Förmåga att frambringa och uppfatta rytm, tonhöjd och klangfärg.
Interpersonell intelligens	Förmåga att urskilja och på ett lämpligt sätt reagera på andra människors sinnesstämning, temperament, bevekelsegrunder och önskningar.
Intrapersonell intelligens	Att ha tillgång till sitt eget känsloliv och ha förmåga att urskilja sina känslor och att känna till sina egna starka och svaga sidor.

Tabell 2.2: Intelligenser enligt Armstrong

> *flexible enough to enable the needs of high performers or talented students to be met."*

Trots denna uppmaning har Finland ingen uppdelning i skolorna för stödundervisning av begåvade elever. Resurser finns inte för att både kunna stöda de svaga och de starka eleverna. Finland har därför valt att satsa på de svaga eleverna, vilket gör att vi får fina resultat i bland annat PISA-undersökningarna, men vilket inte gynnar de särbegåvade eleverna. Givetvis så visar inte de akademiska undersökningarna något om stödet som ges, eller inte ges åt elever med särbegåvning inom bland annat idrott och konst.

2.1.2 Begreppet särbegåvning inom matematiken

Man tror kanske att definitionen av matematiskt särbegåvning är enkel. Elever som räknar snabbt, effektivt och rätt brukar bland såväl föräldrar, som lärare anses vara matematiskt begåvade. Men räcker det verkligen för att vara matematiskt särbegåvad? Vilka egenskaper bör en matematiskt särbegåvad elev ha?

Krutetskii (Krutetskii, 1976) genomförde en tolv år lång undersökning gällande barns matematiska förmågor. Enligt honom finns det en viss sorts struktur för den matematiska förmågan. Nedan finns listat de tre punkter som han själv poängterar. Om man behärskade alla dessa tre, samt hade ett *matematiskt sinnelag* hade man enligt Krutetskii en begåvning inom matematiken.

- förmåga att samla in matematisk information
- förmåga att bearbeta den insamlade matematiska informationen
- förmåga att bevara den matematiska informationen

Pendarvis, Howley & Howley (1990) har senare utökat och omarbetat något på Krutetskiis påståenden. Enligt dem kan man se på punkten om samlandet av matematisk information på ett lite annat sätt. Denna punkt beskriver enligt dem en förmåga hos elever att snabbt förstå innebörden av en matematisk fråga, samt hur man bäst borde gå till väga för att lösa den. När det senare gäller att bearbeta den matematiska informationen anser Pendarvis mfl. att matematiskt begåvade elever inte bara finner en lösning på ett problem, utan ofta kan finna flera olika sätt att lösa samma problem på.

Det som verkar vara den allmänna uppfattningen är, med andra ord, inte nödvändigtvis bara det att särbegåvade elever är snabba på att räkna, utan fokusen ligger mera vid det matematiska sinnelaget. Att vara så kallat skolsmart, betyder inte att man är matematiskt särbegåvad, trots att man säkert har en viss fallenhet för ämnet. Elever kan mycket väl få fina vitsord i matematik, utan att faktiskt vara särbegåvade i ämnet. (Lehtonen, 1994) Detta tar oss obestridligt till nästa problem, nämligen hur urskiljer vi då de matematiskt särbegåvna?

Hur urskiljer man elever med matematisk särbegåvning

Då Pettersson (2008) gjorde en enkätstudie bland lärare för att bland annat kartlägga deras syns på matematisk förmåga, fick hon en väldigt snäv och något snedvriden syn till svar från dem. Endast de elever som räknade snabbt, var aktiva och jobbade självständigt ansågs vara särbegåvade. Enkätstudien innehöll svar från förskolan fram till nionde klass, men eftersom mitt eget material är ämnat för niondeklassister så väljer jag att citera lärare från årskurserna 7-9.

> *Lyckas bra på prov. Snabbt klara med uppgifter och visar att de förstår det de gör. Aktiva vid genomgångar, pigga på att diskutera matte, vetgiriga.*

> *Hur de uttrycker sig muntligt. Hur snabbt de löser olika problem som är nya för dem. De säger att det är lätt.*

Elever med särbegåvning inom matematik kan mycket väl hittas genom att söka efter dessa färdigheter, men det är inte uteslutande aktiva och snabba elever som kan vara särbegåvade. Det är också här ett stort problem uppstår när man vill urskilja dem. De snabba och aktiva är lätta att hitta, men hur är det med de som visar sitt matematiska sinnelag på annat sätt?

Till skillnad från till exempel idrott, där särbegåvning ses som något beundrandsvärt bland klasskamraterna, så ses matematisk särbegåvning ibland som något ”töntigt” och ”nördigt”. Detta leder till att elever med särskild fallenhet för matematik inte vill visa sina

kunskaper för att inte bli utesluten ur gruppen. Dessa elever kommer varken vara särskilt snabba eller aktiva under lektionen, men är likväl matematiskt särbegåvade.

Både Bates & Mundy (2005) och Barger (1998) har skapat listor över karaktärsdrag de anser vara riktgivande för finnandet av matematiskt särbegåvade elever. När jag själv jämför dessa listor med karaktärsdrag så finner jag förvånansvärt hur de kompleterar varandra, utan att faktiskt ta upp samma karaktärsdrag. I tabellen 2.3 finns till höger Bates & Mundys karaktärsdrag sammanfattade av Petterson (2008) och till vänster Bargers karaktärsdrag sammanfattade av Eriksson (2010).

Barger	Bates & Mundy
Lätt för att räkna	Tidig förmåga att uttrycka sig och samtala med vuxna
Lätt för att associera	Brett ordförråd och utmärkt läsförmåga
God taluppfattning	Orubblig nyfikenhet och frågvishet
Skapar egna metoder till svåra uträkningar, men har svårt att förklara hur de kom fram till svaret, de bara vet att det är rätt	Förmåga att tänka abstrakt, uttrycker komplexa idéer och tankar
De blir ofta förvånade över att inte alla tycker att svaret är självklart	Föredrar att umgås med äldre eller vuxna, har ibland svårt att hitta vänner i sin egen ålder
De lär sig på egen hand, letar efter mönster och kan i en tidig ålder resonera abstrakt	Ett utmärkt minne, förmåga att bevara och använda information i nya situationer
De försöker förändra regler och förslår lösningar som skiljer sig från de som normalt lärs ut	Ett sinne för humor som kan betraktas som något udda av andra
De hittar kopplingar mellan nya och gamla kunskaper och vill ständigt veta varför	Utmanande beteende, särskilt då de är uttråkade eller frustrerade
	Otålighet över skolarbetet som de tycker saknar faktisk mening

Tabell 2.3: Karaktärsdrag för matematiskt särbegåvade enligt Berger och Bates & Mundy

Denna lista kan åtminstone hjälpa lärare att urskilja de särbegåvade eleverna, vilket kan vara särskilt viktigt för de nyare lärarna. Enligt Männistö (2013) så har nämligen nyblivna lärare mycket svårare att märka av särbegåvade elever än mera erfarna lärare har. Lehtonen (1994) säger också att lärare behöver fortbildning i hur man urskiljer särbegåvna elever, för att verkligen kunna fördjupa sig i de olika särbegåvningarna och deras särdrag. Förutom att lärarna självständigt ska försöka finna de särbegåvade eleverna under lektionerna, så är det mycket viktigt att de också samarbetar tillsammans med föräldrarna. (Dean, 2006) Genom att samarbeta med föräldrarna så kan man som lärare lättare få insikter i deras styrkor och svagheter, samt lättare urskilja om karaktärsdragen man ser under lektionen också är vanliga i hemmet. Endast när man urskilt en särbegåvade elev, kan man börja

undervisa eleven enligt hens behov.

2.1.3 Undervisning av särbegåvade elever

När en särbegåvad elev sist och slutligen urskiljs måste man som lärare börja fundera kring hur man bör undervisa en sådan elev. Faktum är att precis som en elev med mycket svårigheter med matematik behöver särskilt stöd för att utvecklas, behöver också en särbegåvad elev speciellt anpassad undervisning för att avancera med sitt lärande. Elever som får utforska sin matematiska gränser och pröva på svårare teman inom matematiken har en större sannolikhet att lyckas med sina matematiska studier i senare utbildning (Smith, 1996). Många av de särbegåvade eleverna finner också skoltiden tråkig och kan därmed också underprestera, eftersom de inte finner motivationen att studera då allt enligt dem är för enkelt (Eriksson, 2010). För att särbegåvade elever inte ska bli uttråkade bör särbegåvade elever få möjlighet till bland annat mer krävande material för att bli såväl inspirerade och utmanade (Ruokamo, 2000).

Lärare har sällan varken tid eller resurser för att verkligen satsa på de särbegåvade eleverna, eftersom mycket av tiden går till att stöda de elever som har svårigheter istället. I Finland får man inte heller dela upp klasser i högstadiet enligt kunskapsnivåer, vilket troligen skulle gynna de elever som har fallenhet för matematik. När man läser läroplanen (Utbildningsstyrelsen, 2014) så finner jag inte någon plan för särskilt begåvade elever, medan elever med svårigheter kan få tre olika sorters stöd allmänt, intensifierat, eller särskilt stöd och därmed individualiserad läroplan. Detta ger enligt mig en bild åt lärare att endast de svaga eleverna ska komma i fokus och få sin egen individuella plan. Det är dock väldigt viktigt att även särbegåvade elever får ett skräddarsydd plan för lärandet (Goodhew, 2009).

Mycket av dagens undervisning i Finland går ut på att lösa rutinuppgifter och räkna tyst i klassrummet, vilket bland annat den nya läroplanen försöker ändra på. Med denna väldigt klassiska syn på hur matematik undervisas, gynnas inte särbegåvade elever. Det resulterar nämligen i att de oftast får fortsätta att räkna rutinuppgifter, fast med svårare tal, när de är färdiga med sina urspungliga uppgifter och vill få nya utmaningar. Det har visat sig att elever med särskild begåvning istället skulle vara i behov av projektarbeten och egna helheter (Viro, 2014). Särbegåvade elever måste också få använda sin egen fantasi för att lösa uppgifter, inte bara följa givna modeller (Ruokamo, 2000). Yli-Sikkilä (2014) som fokuserat på att bearbeta material för särbegåvade elever inom matematiken anser också att tillämpad problemlösning är att föredra i deras undervisning. Om man undersöker läroplanens mål för specifikt matematik och inte i allmänhet, så finns där ett kort sammandrag om handledning, differentiering och stöd där de enligt mig tagit fasta på detta behov.

> *Undervisningen kan berikas genom att fördjupa det innehåll som behandlas gemensamt enligt elevernas intresse och kunskapsnivå. Skickliga elever ska stödjas med hjälp av alternativa arbetsformer, till exempel olika projekt*

och problembaserade undersökningsuppgifter inom matematiska områden som intresserar dem.

Det forskare kan vara ense om är alltså att elever med särbegåvning är i behov av särskilt stöd. Forskare har också hittat olika sätt att undervisa särbegåvade elever för att de ska utvecklas så mycket som möjligt, bland annat med problemlösning. Det som det dock finns väldigt lite av är konkreta material och anvisningar för hur man borde undervisa särbegåvade elever. Detta resulterar i att lärarna själva blir tvungna att skapa material, vilket är mycket slitsamt och tidskrävande. Detta resulterar i att materialen sällan skapas och eleverna istället får räkna andra uppgifter ur den vanliga matematikboken, men av en större svårighetsgrad. Lärare sätts också inför dilemmat att undervisa elever med behov av särskilt stöd på grund av svårigheter och särbegåvning samtidigt. E-läromaterialet som jag skapat är skapat just för att underlätta lärarens arbetsdag med just detta dilemma. E-läromaterialet avser att ge eleverna ett helhetsbaserat ämne att jobba med som lärarna inte själv behöver skapa. Efter att nu ha definierat ordet särbegåvning kommer jag att fortsätta med att definiera hur ett e-läromedel ser ut och varför det kan vara nyttigt att använda sig av e-läromedel i undervisningen.

2.2 Användning och definiering av ett e-läromedel

Utbildningsstyrelsen har publicerat materialet, "*Med kvalitet i fokus - E-läromedlen i undervisning och lärande*", som förklarar vilka faktorer som gör ett e-läromedel bra. Jag tänker jämföra mitt eget e-läromaterial med det jag hittat i dokumentet och redogöra för de förändringar jag gjorde och inte gjorde baserat på Utbildningsstyrelsens material. Jag kommer också att kort redogöra för orsaker att använda e-läromedel i sin undervisning, samt fundera på möjligheterna som e-läromedlet ger till distansundervisning.

2.2.1 Hur ser ett bra e-läromedel ut?

Enligt Ilomäki (2012) finns det många olika klassificeringar av e-läromedel. Exempel på några av dessa är utvärdering, blogg, kunskapskälla, wiki, spel och demonstrationer. Hemsidor kan också fungera som ett e-läromedel och därför valde jag att skapa just en sådan. När jag kollar på mitt eget e-läromaterial och de olika klassificeringarna som finns så inser jag snabbt att mitt material är en blandning av många utav klassificeringarna. De tre klassificeringar som passar e-läromaterialet bäst är: öppen aktivitet, kunskapskälla och material som stöder undersökande lärande. Det här betyder alltså att mitt e-läromaterial innehåller material som förklarar olika fenomen, men att det också finns olika sorters uppgifter som stöder lärandet av teorin som behandlas. Enligt en annan klassificering som också tas upp i artikeln så är mitt e-läromaterialel en temahelhet, vilket betyder att den behandlar endast ett tema, temat i detta fall är kryptografi.

Ilomäki (2012) har satt upp några riktlinjer för hur ett bra e-läromaterial bör se ut:

Det kan användas flexibelt enligt elevens kunskapsnivå, intresse och behov, det stöder kollaborativt, långsiktigt arbete, aktiverar elevens tänkande, fokuserar på kärnfrågorna i det fenomen som studeras och stöder utvecklingen av förmågan att lära sig. Funktionsmässigt är ett bra e-läromedel tekniskt lätt att använda och visuellt stöder det de pedagogiska och innehållsmässiga målen.

Det finns också närmast ett överflöd av e-läromedel på nätet att använda sig av. Trots att det finns mycket olika gratismaterial på nätet så är det väldigt få lärare som använder sig av dem (Ilomäki, 2012). Största orsaken till detta är att de inte vet hur materialen ska användas. Det är alltså viktigt att materialet är lätt att använda för såväl eleverna som lärarna. Om läraren inte förstår hur materialet ska användas, så kommer inte heller eleverna få en chans att testa på det. När det gjordes en undersökning gällande lärares användning av e-läromedel i undervisningen visade det sig att endast en bråkdel av lärarna verkligen använde sig av e-läromedel på ett smidit och mångsidigt sätt. Största delen av lärarna gjorde det inte och en av anledningarna som nämndes var att de inte kände att de hade tillräckliga IT-färdigheter. För att lärare ska kunna använda sig av materialen som ges dem, måste de därför vara väldigt lätt att använda, eller sedan måste det erbjudas tillräcklig fortbildning för att lärarna ska kunna lära sig använda materialet.

Med detta i åtanke var jag alltså tvungen att skapa ett tekniskt enkelt material som kan användas utan några särskilda förkunskaper. Det gjorde att jag sist och slutligen valde att skapa ett e-läromaterial i Google-sites, vilket i praktiken betyder att jag skapar en hemsida. Hemsidor är i dagens läge något som de flesta kan använda sig av och det enda man behöver kunna är byta flik och då får de upp nästa kapitel i materialet. För att ännu förenkla användningen har jag på förstasidan skrivit ner en kort sammanfattning hur man använder sig av materialet. Det som dock återstår som problem är hur lärarna ska hitta materialet i djungeln som kallas internet. Jag valde därför att skicka länken till rektorerna av en del svenskspråkiga skolor och be dem vidarebefodra länken till matematiklärarna. Genom att ta direktkontakt med dem hoppas jag att lärarnas tröskel att testa på materialet sjunker. Om mitt material är bra enligt lärarna som använder det, tror jag att det naturligt kommer att spridas.

Enligt Jaakola, Nirhamo, Nurmi och Lehtonen (2012) så finns det ingen ideal längd eller storlek på ett material. Små material är lätta att kombinera med annat, medan större material lättare kan användas som helhet. Jaakola, Nirhamo, Nurmi och Lehtonen (2012) påstår ännu att ett omfattande material hellre används av lärare som är oerfarna vad gället teknologi. Jag har därför valt att göra ett material som är någon sorts medelväg, genom att göra den till en temabaserad helhet. Det är inte särskilt långt, men eftersom tanken är att vissa elever endast kommer att ha en kortare stund på sig att verkligen arbeta med det så blir det tillräckligt långt för att ta upp största delen av läseåret. Om man dock väljer att jobba med detta material som en helhet med klassen, vilket självfallet går, så kan man räkna med att varje del av materialet kan gås igenom på en lektion på 45 minuter. Detta betyder att man skulle gå genom materialet på ca sju lektioner, vilket skulle göra detta till ett kort material.

Materialet är som tidigare nämnt riktat åt särbegåvade elever och jag valde därför att speciellt fokusera på stöd av expertmässigt arbete. Ilomäki (2012) nämner att forskning tyder på att elever borde få uppmuntras att ta på sig rollen av en expert och få testa på krävande uppgifter. Tanken är att eleverna skilt för sig eller tillsammans tar på sig uppgifter som blir gradvist svårare för att på detta sätt utvecklas till experter. Ett sådant tillvägagångssätt främjar elevens förståelse för materialet. Istället för att bara memorera fakta lär sig eleverna att tillämpa kunskaper de har från tidigare för att lösa nya problem. Ilomäki (2012) räknar upp fyra punkter för e-läromedel som kan hjälpa det främja expertundervisning.

- Använd problem och utmaningar i det verkliga livet
- Vägled eleverna att använda sin expertkunskap
- Ge expertmodeller
- Hjälp och vägled enligt situation

Jag har försökt förverkliga dessa punkter i mån av möjlighet i mitt e-läromaterial. Genom att se till att en del av uppgifterna är direkt kopplade till vardagen hoppas jag att de ska finna att uppgifterna som ges är viktiga i framtiden. Ett bra e-läromedel ska vägleda eleverna att använda sin expertkunskap. Detta tycker jag att jag lyckats med väldigt bra i skapandet av mitt eget e-läromaterial. Genom att dela upp e-läromaterialet i olika kapitel har jag lyckats skapa olika kärnfrågor som bör redas ut innan man kan komma till den stora huvudfrågan, vilket i det här fallet är RSA. Genom att sätta upp delmoment har jag försökt få eleverna att se hur små saker som man kan tycka är lätta, bygger upp till något som kan tyckas vara matematiskt svårt, men för dem nu är ganska enkelt. Genom delmomenten får eleverna en chans att lyckas, vilket alltid är mycket viktigt. Detta gör, att fastän det sista kapitlet är svårt och kanske för krävande, så har eleverna lyckats bygga upp ett självförtroende i lösandet av de andra uppgifterna.

Expertmodellerna och vägledningen har dock varit de svåraste punkterna att uppfylla. Vägledningen har jag försökt skapa genom att till en del av de svårare uppgifterna sätta med lösningstips. Det finns också exempeluppgifter till de lättare uppgifterna så att eleverna får en modell att följa. Det som eventuellt ännu skulle ha hjälpt med vägledningen skulle ha varit ett givet facit till uppgifterna. Jag har dock valt att inte sätta med ett facit av andra orsaker. Expertmodellerna har varit svårast och jag anser att jag endast fått med det med hjälp av modellexemplen.

Det har tidigare nämnts att elever med särbegåvning ofta finner skoltiden långtråkig och trist. Det är därför ytterst viktigt att kunna motivera eleverna för att hålla upp deras intresse. Ativiteter som inte vanligtvis hör till undervisningen kan bland annat fungera som motivationshöjare Tapola & Veermans (2012). Men i slutändan kan sådana aktiviteter vara kortavariga motivationshöjare och man måste hitta sätt att långvarigt få elever motiverade. Varför borde man då använda ett e-läromedel för att höja motivationen?

- Man kan dra nytta av e-läromedlets stimulerande egenskaper
- Det kan erbjuda individuella och alternativa lärovägar
- Man kan dra nytta av återkoppling under arbetet
- Det erbjuder motiverande stöd under hela lärprocessen

Förutom att skapa ett motiverande material har jag också försökt skapa ett material som tar upp problem och situationer som är vanliga i samhället. Enligt Jaakkola (2012) är det viktigt för elever att inse komplexiteten av ett samhälleligt fenomen och fundera kring det, istället för att lösa klassiska läroboks problem. Detta för att elever ska få en realistisk bild av samhället och hur vuxenlivet kommer att kunna se ut. Lösningen till ett problem leder ofta till ett annat problem istället för att bara ge en tillfredställande lösning (Jaakkola, 2012). Jag har försökt implementera detta tankesätt i mitt e-läromaterial genom att fokusera på de punkter som Jaakkola (2012) nämner gällande komplexitet och mångsidighet.

- Förankra problemen i verkligheten
- Sporra eleverna att tänka på fenomenet
- Hjälp eleverna att förstå fenomenets komplexitet
- Sammankoppla problemen med elevens erfarenhetsvärld
- Stöd fördjupad behandling av fenomenet
- Presentera fenomenten mångsidigt och på flera nivåer
- Använd flera framställningssätt för att belysa fenomenet

Jag anser att jag lyckats väldigt bra med att förankra problemen i verkligheten, genom att välja temat kryptografi. I dagens samhälle är kryptografi något som blir viktigare och viktigare med tanke på stora samhälleliga frågor som till exempel dataskydd. Jag har också varit mycket noga med att försöka sammankoppla mitt material med elevens erfarenhetsvärld, genom att noggrant fundera på vilken årskurs materialet lämpar sig till, samt se till att de har tillräckligt med förkunskaper för att kunna ta till sig materialet. Genom att skapa uppgifter där eleverna själva måste söka information har jag försökt sporra eleverna att såväl tänka på fenomenet som helhet, som stöda dem att fördjupa sig i fenomenet. Nivåuppdelnigen av materialet kom väldigt naturligt, med hjälpa av kapitelindelningen. I varje kapitel får eleverna ta till sig ny information, samtidigt som de får använda sig av tidigare kapitel för att lösa problemen. Att skapa flera framställningssätt för att belysa kryptografi har dock varit svårt. Största utmaningen för mig var att skapa ett material som hade visuellt stöd. De bilder jag kunnat använda mig av är sådana som

finns som öppet delade bilder på nätet. Detta ger en väldigt mycket restriktioner kring vad som går att använda och vilken kvaliteten av dessa bilder är. Jag anser dock att bilderna jag hittat underlätttat förståelsen för fenomenen som de beskriver.

Sammanfattningsvist så anser jag att jag tagit mycket av föreslagen till ett bra e-läromedel i beaktande när jag skapade mitt e-läromaterial och lyckats förverkliga åtminstone en del av dem. Största utmaningarna har varit mina egna kunskaper i datateknik, samt möjligheterna som ges via Google sites. Skapandet av ett mångsidigt och användbart e-läromaterial har varit betydligt svårare än vad jag först föreställde mig, trots det skulle jag i framtiden kunna tänka mig skapa liknande hemsidor. En av de främsta orsakerna till att skapa flera e-läromaterial är möjligheterna de skapar till bland annat distansundervisning.

2.2.2 Varför använda e-läromedel?

Tidigare har jag nämnt hur resursbrister påverkar lärarnas förmåga att stöda de särbegåvade eleverna. Resursbristen påverkar inte bara lärare, utan i vissa fall hela skolor. Små gymnasier vid landsbygden kan i vissa ämnen redan ha svårt att erbjuda valbara kurser åt sina elever på grund av resursbrist, men i och med detta har också distanskurser blivit vanligare. Det visar sig också att distanskurser kan ha en positiv inverkan på elevernas skolgång (Olszewski-Kubilius & Lee, 2004). Wallace (2009) påstår dessutom att distansundervisning kan främja specifikt begåvade elevers inlärning, eftersom kursen kan erbjuda säkerhet och tillgänglighet på ett annat sätt än den vanliga närundervisningen kan.

Eftersom mitt e-läromaterial är en hemsida som är öppen på internet går det att använda det som ett distansmaterial. Det finns alltid nu som då elever som av olika orsaker inte deltar i skolgången. Vid sådana tillfällen så kan ett distansmaterial vara till mycket nytta. Problemet med just mitt eget e-läromaterial är givetvis att det inte är en del av läroplanen och därmed inte kan ersätta vanlig matematikundervisning. Mitt e-läromaterial kan istället användas av begåvade elever som vill jobba på distans under sin egen fritid.

Samhället går hela tiden framåt och det går inte mera att blunda för den snabba framfart teknologin har. Undervisningen måste därmed också utvecklas. Distansundervisning, e-läromedel och e-läromaterial är konkreta sätt som undervisningen försöker hänga med i samhällsutvecklingen. Tidigare har till största del endast allmänheten stöttat e-undervisningen, men på senare tid har även pedagogiken öppnat ögonen för användningen av e-lärande (Álvarez, Moreno, Orduna, Pascual & san Vicente, 2015). Även eleverna håller sig positivt inställda till e-läromedel, men många elever poängterar fortfarande behovet av papper och penna (Galbraith & Haines, 1998). Det finns med andra ord många orsaker att fortsätta utveckla och använda sig av e-läromedel. Det är också något vi i Finland har tagit till oss och försöker uppmuntra bland annat i den nya läroplanen.

2.3 E-materialets grunder i allmänna läroplanen

År 2014 togs den senaste läroplanen i avändning i skolorna. Den var något kontroversiell, eftersom den förespråkar bland annat mer elevcentrerad undervising än tidigare. Dagens

läroplan är uppdelad i sju stycken olika kompetenser, varav digital kompetes är en av dem. Dessa sju kompetenser ska forma lärarnas undervisning i hopp om att eleverna ska uppmuntras till livslångt lärande. I tabellen 2.4 finns uppräknat de sju kompetenserna, samt en kort förklaring av deras betydelse.

Kompetenser	Sammanfattning
Förmåga att tänka och lära sig (K1)	Eleverna ska bland annat uppmuntras att söka information och lära sig att använda sig av tidigare kunskap för att ställa sig kritisk till den nya informationen. De ska också få testa på olika sätt att lära sig, för att hitta de lärmetoder som passar dem bäst.
Kulturell och kommunikativ kompetens (K2)	Eleverna ska lära sig att identifiera olika kulturella fenomen och själva hitta sin individuella kulturella identitet. De ska få en positiv inställning till omvärlden och lära sig kommunicera med den på ett respektfullt sätt.
Vardagskompetens (K3)	Eleverna ska lära sig hur de ska överleva i den ständigt ändrande vardagen. Hit hör många olika färdigheter, bland annat trafik, motion, teknologi, samt ekonomi och konsumption.
Mulitilitteracitet (K4)	Eleverna ska klara av att tolka, producera och förstå texter i olika miljöer. Texterna kan vara framställda på olika sätt, bland annat skriven, talad eller digital.
Digital kompetens (K5)	Eleverna ska få möjlighet att utveckla sina digitala kunskaper och digitala verktyg ska systematiskt vara del av deras undervisning.
Arbetslivskompetens och entrepenörskap (K6)	Elevernas intresse för arbete bör främjas och de bör få erfarenheter kring arbete och näringsliv.
Förmåga att delta, påverka och bidra till en hållbar framtid (K7)	Eleverna ska få förståelse för sina demokratiska rättigheter, friheter och skylldigheter. Skolan ska också handleda elever att bli medborgare som förstår konsekvenserna av sina handlingar på såväl naturen, samhället och egna livet.

Tabell 2.4: Läroplanens kompetenser med sammanfattningar

Eftersom dessa kompetenser är stöttestenarna för läroplanen försökte jag i mån av möjlighet implementera dem i mitt eget e-läromaterial. Första kompetensen K1, anser jag att väldigt naturligt blir en del av mitt e-läromaterial, eftersom tanken är att eleverna självständigt ska jobba med det. Jag behövde alltså inte anpassa mitt e-läromaterial på något vis för att lyckas fläta in K1. Det blev dock desto svårare att försöka få med kompetens K2 i mitt e-läromaterial. Jag lyckades inte uppfylla K2 på något konkret vis, men det man kan tänka sig är att matematik i sig är kulturellt och på så vis uppfyller K2. Däremot kan man gott och väl tänka sig att kompetensen K3 är en del av mitt

e-läromaterial. E-läromaterialet är en del av paraplybegreppet teknologi, vilket specifikt nämns som ett mål i K3. Komptenserna K4 och K5 är återigen båda två väldigt naturliga delar av mitt e-läromaterial. K4 poängterar texter i olika former, däribland digitala, medan hela K5 förespråkar digitalt kunnande. Såväl K6, som K7, har jag tyvärr blivit tvungen att lämna bort från mitt e-läromaterial, eftersom jag inte lyckade få det inbakat i materialet på något vettigt sätt.

Om man kollar på helheten så följer mitt e-läromaterial många av läroplanens riktlinjer för den allmänna undervisningen, men eftersom e-läromaterialet är skapat för matematikundervisningen vill jag ju självfallet att den ska följa de allmänna riktlinjerna för det ämnet också. Enligt läroplanen (Utbildningsstyrelsen, 2014) har matematiken bland annat följande uppdrag som läroämne:

> *Uppdraget i undervisningen i matematik är att utveckla ett logiskt, exakt och kreativt matematiskt tänkande hos eleverna. Undervisningen ska lägga grund för förståelsen av matematiska begrepp och strukturer samt utveckla elevernas förmåga att behandla information och lösa problem. På grund av matematikens kumulativa natur ska undervisningen framskrida systematiskt. Konkreta och laborativa inslag är centrala i undervisningen och studierna i matematik. Lärandet stöds med hjälp av informations- och kommunikationsteknik.*

Återigen uppfyller mitt e-läromaterial nästan alla kriterier. E-läromaterialet försöker uppmuntra elever att behandla information och lösa problem, dessutom att själv söka upp informationen och stå sig kritisk till den. Uppbyggnanden av e-läromaterialet förutsätter också ett väldigt systematisk arbete, helt i enlighet med läroplanens uppdrag. Väldigt naturligt så stöds undervisnigen av informations- och kommunikationsteknik om e-läromaterialet används i undervisningen. Därmed kan jag dra slutsatsen att e-läromaterialet är motiverat ur läroplanssynvinkel.

Sammanfattningsvist har vi särbegåvade elever i Finland som är i behov av speciellt stöd för att deras inlärning ska främjas. Det finns många olika sätt att uppnå detta, men enligt forskning är e-läromaterial ett mycket användbart redskap för att uppfylla stödundervisningen. Jag valde därför att skapa ett e-läromaterial, vars tema står utanför läroplanen. Trots att temat inte nämns, så uppfyller e-läromaterialet dock många av läroplanens mål och uppdrag och kan därför motiveras att användas i undervisningen.

Presentation av e-läromaterialet

Avsikten är att i detta kapitel presentera e-läromaterialet och förklara hur jag själv har tänkt att det ska användas. Jag kommer att ta upp alla kapitel i e-läromaterialet skilt för sig och utifrån det ge flera olika användningssätt för varje kapitel. Orsaken till att jag går igenom dem kapitelvis är att en del av e-läromaterialet är väldigt matematikinriktat och en del går att användas i ämnesöverskridande undervisning. När jag presenterar e-läromaterialet kommer jag hänvisa till hemsidan, vilken jag satt med som bilaga längst bak. E-materialet baserar sig som tidigare nämnt på grunderna i kryptografi. Den finns att besöka på webbadressen: https://sites.google.com/view/kryptografi/ och är skapad med hjälp av Google Sites.

3.1 Introduktion

Det har visat sig att särbegåvade elever ofta finner sin skolgång som långtråkig och inte alltför givande. Detta eftersom de oftast inte får den sorts utmaning som krävs för att stimulera dem. Som tidigare nämnts behöver också särbegåvade elever särskilt stöd och särskilt planerade uppgifter för att kunna utvecklas matematiskt. E-läromaterialet är skapat för att ge eleverna en utmaning i att lära sig något nytt och dessutom själva vara ansvariga för sin egen inlärning.

Ett av de största problemen med att ge de särbegåvade eleverna den uppmärksamhet och svårighetsgrad de behöver är tidsbrist hos lärarna och ekonomiska orsaker. Den ekonomiska aspekten är lätt att klara upp genom mitt e-läromaterial. Med e-läromaterialet behöver inte lärarna själva skapa något och eftersom det är gjort via Google Sites är det också gratis på nätet. Tidsbristen hos lärarna är dock ett svårare problem. Genom att göra e-läromaterialet lätt tillgänligt behöver lärarna inte själva skapa ett material, men som med allt krävs det förstås att lärarna går genom e-läromaterialet grundligt för att hitta dess användningsområden. Lärarna skall dock inte behöva ha en väldigt aktiv roll i undervisningen med hjälp av e-läromaterialet, eftersom tanken är att eleven på egen hand ska läsa materialet och göra uppgifterna. Detta ger lärarna möjligheten att fokusera på de elever som behöver speciellt stöd.

Tanken med e-läromaterialet är att eleverna lätt ska komma åt teorin och uppgifterna efter att de har blivit klara med uppgifterna som blivit givna åt dem av lärarna. Detta händer ofta med särbegåvade elever och är som tidigare nämnt också ett av karaktärsdragen hos särbegåvade elever. De blir ofta klara snabbare än de övriga eleverna och får ofta vänta på att de andra blir klara. Om läraren hinner kan hen ge extra uppgifter till eleven, men dessa uppgifter är oftast liknande till sådana som eleven gjort, men med andra siffror. Om eleven redan förstått konceptet kan det kännas långtråkigt för hen att göra samma uppgifter igen. E-läromaterialet erbjuder alltså eleverna något helt nytt, i förhoppningen

om att höja deras motivation att arbeta.

E-läromaterialet är som jag tidigare nämnt en hemsida uppbyggd med Google sites. Varje flik innehåller material som bygger upp temahelheten kryptografi. Jag tänker mig varje flik som ett enskilt kapitel. Kapitlen innehåller teori samt uppgifter för eleverna att lösa. Jag har dock valt att inte sätta med ett facit till uppgifterna, eftersom tanken är att eleverna själva ska inse om svaren är rätt eller fel. Detta kan vara ganska svårt, men är en väldigt bra och uppbyggande övning för dem. Om man kan motivera att en uppgift är klar och rätt, så är den troligen det. Jag har också valt att endast ha ungefär fem uppgifter per kapitel. Detta av två orsaker. Den första är att de under en kort del av lektionen knappast kommer hinna göra särskilt många uppgifter och då är det också onödigt att ha massor av dem. Den andra orsaken är att jag tänkte att med färre, lite mer tidskrävande uppgifter så skulle intresset vara större än med många korta. Förhoppningen är att de inte ska hinna sätta in sig i mer än en högst två uppgifter per lektion, efter att de blivit klara med arbetet läraren gett dem.

Hemsidans första sida innehåller en mycket kort förklaring över användningen av materialet. Bilaga 1 visar hur första sidan ser ut. Eleverna ska från första sidan enkelt kunna förflytta sig till nästa kapitel, genom en av flikarna som finns på hemsidan. Tanken är att eleverna ska arbeta genom varje kapitel i ordningen som ges, eftersom kapitlen bygger på varandra. Första kapitlet kommer att presenteras nedan.

3.2 Kryptografi

E-läromaterialet börjar med att likna något som eleverna kanske tänker sig som icke-matematisk. Det finns inga räkneuppgifter och inte heller någon teori gällande den matematik som tas upp. Detta är ett helt medvetet val för att visa att matematik kan kopplas till många andra ämnen. Kapitlet ger en introduktion till vad kryptografi egentligen handlar om, samt dess historia och användningen i dagens samhälle. Uppgifterna som hör till kapitlet ger eleverna möjligheter till väldigt mycket variation. Eleverna får bekanta sig med olika kodspråk och de grundläggande begreppen inom kryptografi. De resterande uppgifterna, vilka man kan se i Bilaga 2 är till för att skapa ett samband mellan kryptografi och elevernas vardag.

E-läromaterialet är också skapat för att kopplas till andra ämnen än bara matematik. I detta kapitel så görs de starkaste kopplingarna till modersmål och historia. Materialet kan alltså användas för att hålla en ämnesöverskridande lektion med något av dessa ämnen om man så önskar. Kodspråken kan kan kopplas ihop med språkuppbyggnad, vilket alltså betyder modersmålsundervisning och Enigma-maskinen och spioneri är direkt kopplade med andra världskriget.

När jag jämför detta kapitel med anvisningarna för hur ett bra e-läromaterial ser ut märker jag att kapitlet uppfyller mycket av anvisningarna. Bland annat har jag försökt att förankra problemen i verkligheten och försökt sporra eleverna att tänka på fenomenet. Kapitlet kan också sammankopplas med specifika kompetensmål i läroplanen. De två

kompetenser som genomsyrar kapitel mest är vardagskompetens och förmågan att tänka och lära sig själv. Multiliteracitets kompetensen kan man också tänka sig att är en del av detta kapitel, speciellt om tänker på uppgift tre, vilken man kan titta på i Bilaga 2.

Tanken bakom det inledande kapitlet är att eleverna ska få en uppfattning om vad kryptografi handlar om och hur denna påverkar dem i det dagliga livet. Det första som e-läromaterialet tar upp i sin teoridel är vad kryptografi verkligen är. För att underlätta begreppet för eleverna har jag tagit till såväl konkreta exempel, som visuell hjälp. E-läromaterialet fortsätter med att ta upp en del av kryptografins historia. Här nämner jag också redan Caesarchiffret, för att väcka nyfikenhet i vad som komma skall. Till sist tar e-läromaterialet upp kodspråk och hur ett sådant fungerar. Eleven har därmed fått ett sammandrag av vad kryptografi är och är sedan redo att gå vidare till nästa kapitel.

3.3 Caesarchiffer

Detta kapitel fungerar som en introduktion till moduloräkning. Det är direkt kopplat till matematik, men eleverna kan fortfarande själva ha svårt att göra den direkta kopplingen. Eleverna ges en kort introduktion till vad ett chiffer är, för att sedan gå vidare till själva teorin bakom Caesarchiffret. För att dekryptera Caesarchiffret ges två olika alternativ. Alternativ nummer två, vilket kan ses i Bilaga 3, är egentligen en direkt användning av modulo. Eleverna är inte medvetna om detta ännu, men jag valde att ta upp Caesarchiffret nu, för att de senare ska kunna skapa ett samband mellan Caesarchiffer och moduloräkning, med andra ord skapa ett samband mellan gammal och ny kunskap. Trots att jag hoppas på att eleverna använder sig av alternativ två när de krypterar med Caesarchiffret, har jag ändå valt att ta upp två olika metoder för att kryptera och dekryptera chiffret. Detta har jag gjort för att visa att problem inom matematiken ofta har fler lösningar än bara en.

Återigen kan man tänka sig att använda detta som ett ämnesöverskridande material om man så vill. Caesarchiffret kan man koppla till undervisnningen om antikens Rom, vilket troligen kan komma upp i historieundervisningen.

Frågorna är denna gång skapade för att på olika sätt undersöka att de lärt sig hur Caesarchiffret fungerar, se Bilaga 3. Det börjar med att de först får kryptera och dekryptera själva. Efter det får eleverna fundera på svagheterna kring chiffret. Denna fråga öppnar upp möjligheten för pararbete om det finns fler än en elev som jobbar med detta kapitel på samma gång. Hela detta kapitel går väldigt bra att jobba par- eller gruppvist. Om eleverna vill jobba utanför materialet går det väldigt bra, genom att t.ex. skriva krypterade texter och försöka lösa varandras krypteringar, eller genom att själva försöka skapa egna chiffer och diskutera dem sinsemellan. Detta kräver dock lite mer handledning från läraren, eftersom inga sådana instruktioner ingår i e-läromaterialet.

Som helhet vill jag med detta kapitel presentera lite matematiskt tänkande och visa konkreta exempel på hur chiffer existerat länge, men med tiden evolverat till det som vi har idag. Jag vill ge dem en mjukstart med matematiken, eftersom jag vet matematiken i e-läromaterialet hela tiden blir svårare och svårare. Detta kapitel uppfyller igen samma

kompetenser från läroplanen som det tidigare kapitlet. Om e-läromaterialet dessutom används som grund för ett par- eller grupparbete så kan man tänka sig att den bygger upp den kulturella och kommunikativa kompetensen.

3.4 Primtal

Primtal borde vara bekant för alla niondeklassister sedan tidigare och jag har därför försökt satsa mera på sådant som inte behandlas i läroböckerna än enbart repetition av primtal. Detta betyder förstås inte att jag helt struntar i att repetera, utan jag har i början en kort teoridel som endast handlar om primtal. Jag har försökt få med ny teori åt eleverna genom ta med en del om primtalsfaktorisering. Teorin som finns i e-läromaterialet går dock att använda istället för en lärobok när man själv undervisar primtal om man så vill. Om man vill variera sin egen undervisning kan man mycket väl ta med primtalsfaktoriseringen i sin vanliga undervisning, eftersom teorin bakom denna inte är överdrivet svår.

Primtalsfaktorisering är inte något som brukar finnas i de vanliga matematikböckerna, men är egentligen bara tillämpning av sådant som eleverna redan borde kunna. Min förhoppning är att eleverna ska få möjligheten att dra kopplingar mellan sådant de kan och sådant som är nytt. Jag har valt att ge två olika exempel på hur man kan lösa uppgifter med primtalsfaktorisering. Sätten är egentligen identiska, men faktorträdet, vilket man kan se i Bilaga 4, är mera visuellt för sådana elever som behöver det. Websidan hade ursprungligen inget faktorträd, men efter att jag läst materialet om hur e-läromaterial borde se ut och fungera, så valde jag att försöka visualisera fenomenet. Detta eftersom Utbildningsstyrelsens utgivna material starkt förespråkade visualisering av fenomen.

Trots att primtal är väldigt matematiskt, så kan man med lite fantasi kunna skapa ämnesöverskridande undervisning också med detta kapitel. Det jag själv tänkt skulle kunna vara något sorts samarbete med bildkonstundervisningen. Det som jag hade i åtanke var ett konstprojekt med faktorträdet som grundidé.

Detta kapitel har jag varit extra noggrann med att använda matematiskt språk. Begreppen faktor, produkt och faktorisering används ofta. Eleverna borde från tidigare veta vad dessa ord betyder, men det är något som de ändå ofta glömmer. Eleverna kommer troligen behöva mera hjälp i att förstå texten, än vad de vanligtvis skulle behöva. Igen kan det vara bra att eleverna jobbar i grupp eller par och tillsammans funderar på vad orden betydde. Alternativt kan de också jobba enskilt, men med att t.ex. börja med att söka rätt på definitoner för de ord de finner svåra.

Uppgiftsantalet har jag igen försökt hålla litet och kompakt för att ge eleverna tid att sätta sig in i dem. Eleverna kan få svar till alla uppgifter, förutom uppgift två, genom att fundera på teorin i materialet. Uppgift två kräver att eleverna själva söker upp information gällande Eratosthenes såll. Det finns väldigt mycket information om detta på nätet och teorin är inte heller så krävande. Jag har valt att ha en svårare uppgift där de själva måste söka information på nätet, eftersom primtal är ett sedan tidigare bekant ämne. Risken finns att eleverna finner uppgifterna för lätta, om de inte kommer något helt nytt som de

måste sätta sig in i på egen hand.

Det som troligen kommer att kännas svårast för eleverna är att förstå varför man går igenom primtal i detta skede. Detta skulle kunna vara något för mig själv att utveckla i framtiden. Hur skulle jag kunna skapa en bra övergång från Caesarchiffer till primtal? Om man direkt från Caesarchiffret skulle gå till moduloräkningen så skulle man se ett väldigt klart samband, men sedan skulle samma problem ändå uppstå, hur kopplar jag smidigt ihop modulo med primtal? Bästa sättet för mig att kunna utveckla på det här är att i framtiden använda mig av e-läromaterialet i min egen undervisning och se hur det fungerar. På det sättet får jag feedback från eleverna och kan senare göra förändringar som underlättar förståelsen för eleverna.

3.5 Kongruensräkning

Vi har nu äntligen kommit till första delen av e-läromaterialet som behandlar något totalt obekant från tidigare för eleverna. Kongruensräkning är väldigt väsentligt för kommande kapitlet om RSA och jag har därför försökt förbereda eleverna så mycket som möjligt med att både förklara om Caesarchiffret och med att jobba lite med primtal. Teorin är uppdelad i två huvuddelar, klockaritmetik och kongruensräkning. Jag funderade länge på att dela upp dessa i två olika kapitel, men valde till sist att låta dem stå tillsammans som ett enda kapitel. Detta är något som jag i framtiden eventuellt kan justera, om det visar sig att eleverna är i behov av två skilda kapitel. Hela kapitlet går att kolla på i Bilaga 5.

Jag börjar med att gå genom hur klockaritmetik fungerar och går sedan vidare till ett exempel. I teoridelen pratar jag om modulo 12 och 24, eftersom dessa är något som de kan koppla ihop mest till sina tidigare kunskaper. I exemplet går jag däremot snabbt vidare till ett annat modulo. Jag har valt att göra så, eftersom eleverna troligen inte kommer ha hur mycket tid som helst under en lektion att jobba med e-läromaterialet, så ju mer jag får in i ett exempel desto bättre. Det kan dock visa sig i framtiden, att det skulle kunna utvecklas till flera exempel, till exempel om klockaritmetik blir ett eget kapitel i e-läromaterialet.

Jag är dock väldigt nöjd med min presentation av kongruensräknningen. Jag bygger min teori på basen av exemplet jag hade om klockaritmetik. Detta hoppas jag ger eleverna en mycket konkretare bild över vad kongruensräkning betyder. Det som jag tror kommer var den svåraste delen för eleverna att förstå är själva modellen för kongruensräkningen. Bokstäver i matematiken kan ibland skrämma bort eleverna från att ens försöka, trots att det egentligen bara förklarar ett fenomen de egentligen redan förstår. Här kan det vara viktigt att läraren tar en lite aktivare roll som handledare för att försöka uppmuntra eleverna att kolla på modellen och försöka förstå hur den ska användas utan att överdramatisera problemet.

Uppgifterna har jag försökt hålla relativt enkela. För eleverna kommer säkert uppgift två att vara den svåraste. Detta eftersom jag inte i min teoridel berättat med exempel hur det fungerar att ha negativa tal som är kongruenta med positiva tal i ett visst modulo. Jag hoppas att det här problemet ska ge eleverna något av en utmaning, men att de

ändå så kunna resonera sig fram till korrekta svar. I skapandet av uppgifterna hade jag kompetens K1 mycket i tankarna. Jag har försökt hitta ett sätt för eleverna att bygga på den information de just fått, genom att kritiskt överväga sina möjligheter. Huvudmålet med speciellt uppgift två är att eleverna försöker resonera sig fram till ett svar, antingen ensam, eller med andra, snarare än att de bara söker efter rätt sätt att lösa uppgiften på via till exempel Google. Efter att uppgifterna är klara så finns det bara ett sista kapitel kvar, RSA-kryptering.

3.6 RSA-kryptering

När eleverna jobbat med alla de tidigare kapitlen som finns till förfogande i e-läromaterialet är det dags för att börja med kapitlet om RSA-kryptering. För att kunna klara av detta utmanande kapitel så krävs det att eleverna studerat de tidigare kapitlen noggrant. Kapitlet är utan tvekan det svåraste, men bygger som tidigare nämnt på matematik som tagits upp tidigare, specifikt på moduloräkning och primtal. Hela kapitlet finns att se i Bilaga 6. För att ge eleverna något av en mjukstart så börjar kapitlet med fakta om RSA-kryptering, snarare än att gå direkt in på teorin.

Kapitlet är i grunden mycket teoretiskt och har formler som eleverna måste kunna tyda. Detta kräver troligen lite mera handledning från läraren, åter en gång. För att försöka förtydliga formlerna så går jag genom ett exempel till alla formler direkt efter att jag gått genom dem. Första delen av teorin bygger på att försöka göra alla uträkningar för nycklarna som behövs för att kunna göra krypteringen. När nycklarna är uträknade går vi vidare till själva krypteringen. I mitt e-läromaterial går jag inte genom varför krypteringen fungerar, eftersom detta är alltför för invecklat för högstadieelever, utan nöjer mig med att visa hur och att det fungerar. När krypteringen är gjord, går e-läromaterialet ännu genom hur dekrypteringen fungerar.

Jag har försökt göra varierande uppgifter gällande temat RSA-krytpering. Först en uppgift för att försöka ge dem en koppling mellan temat vi går genom och deras vardag. Denna uppgift valde jag för att försöka koppla mitt e-läromaterial lite mera till läroplanen. Hela kapitlet är skapat med digital kompetens i åtanke, men jag ville också få med lite annan kompetensbildning och valde därför en uppgift som framhäver bland annat vardagskompetens. Uppgifterna två och tre ger eleverna en chans att använda sig av RSA-krypteringen och dekrypteringen. Sista uppgiften är väldigt krävande på två sätt. För det första så kan det vara utmanande för eleverna att förstå vad som egentligen menas med frågan och för det andra så kräver uppgiften att man kan en del formelberäkning. Formelberäkningar brukar vara svårt för en del högstadieelver, men eftersom tanken är att det är särbegåvade elever som ska jobba med e-läromaterialet tror jag ändå att de kommer klara av det.

Detta kapitel har en väldigt tydlig koppling till datateknik och kan därför enkelt användas i ämnesöverskridande undervisningen av det ämnet. Överlag kan detta e-läromaterial också användas vid undervisning av datateknik, om man undervisar kryptering.

Sammanfattningsvist så bygger e-läromaterialet upp en helhet som kan användas under matematiklektionerna. Fastän tanken är att eleverna går genom kapitlen i ordning, efter att de blivit färdiga med sina egna uppgifter under lektionen, så finns det inget som tvingar en att använda e-läromaterialet så. Alla lärare har själva möjligheten att välja de delar som de vill använda sig av integrera det på valfritt sätt med sin egen undervisning. Lärarna så väl som eleverna har möjlighet att ge förbättringsförslag till e-läromaterialet vartefter användning. På sista fliken på webbsidan finns det möjlighet att skicka in feedback över e-läromaterialet. På detta sätt kommer hemsidan att leva och utvecklas vartefter den används. Bilaga 7 åskådliggör sista fliken av hemsidan.

Matematiken bakom e-materialet

I detta kapitel tänker jag gå genom matematiken som e-läromaterialet bygger på. Här kommer jag ta upp begrepp som delbarhet, primtal, modulo och grunderna till RSA. Jag kommer förklara begreppen och gå genom grunderna till var och en av dem. Alla begrepp som dyker upp i e-läromaterialet kommer i detta kapitel att förklaras och definieras. Som inspiration för mina bevis har jag använt mig av boken *Johdatus abstraktiin algebraan* av Jokke Häsä och Johanna Rämö, samt Anne-Maria Ernvall-Hytönens kursmaterial *Elementär talteori*.

4.1 Delbarhet

Mycket av matematiken som behandlas i e-läromaterialet bygger på delbarhet, även om det inte är ett tema i e-läromaterialet. Därför anser jag att det är ett bra ställe att börja med att definiera delbarhet.

Definition 4.1. Heltalet n är *delbart* med heltalet m, om det existerar ett heltal a så att $n = am$ gäller. Detta betecknar vi $m \mid n$.

Om n är delbart med m kallar vi m för en delare, eller divisor till n. Om n inte är delbart med m så betecknar vi det $m \nmid n$. T.ex. $5 \mid 25$ eftersom $5 \times 5 = 25$, men $6 \nmid 31$, eftersom det inte existerar två heltal vars produkt blir 31.

Eftersom $6 \nmid 31$ betyder det här att när dessa divideras så kommer vi att få en entydig rest. Resttermen brukar betecknas med r.

Sats 4.2. *Låt a och b vara heltal. Vi antar att $b \neq 0$. Då existerar det entydiga $q, r \in \mathbb{Z}$ för vilka gäller att*

$$a = qb + r \ \text{ och } \ 0 \leq r \leq |b|$$

Bevis. Vi börjar med att anta att $b > 0$ och fortsätter genom att undersöka mängden

$$R = \{a - xb \mid x \in \mathbb{Z}\}.$$

Denna mängd innehåller alla tal som skulle kunna vara rester när man dividerar a med b. Det jag tänker bevisa är att den riktiga resttermen är det minsta icke-negativa tal som finns i mängden R.

Vi väljer det minsta icke-negativa talet r ur mängden R. Sådana icke-negativa tal måste existera, eftersom $a - xb \geqslant 0$ om $x \leqslant a/b$. Vi väljer också det heltal q, för vilket det gäller $a - qb = r$.

Vi gör nu motantagandet att $r > |b| = b$. Ifall motantagandet är sant så bör det gälla att

$$a - (q + 1)b = a - qb - b = r - b \geqslant 0,$$

vilket betyder att $a-(q+1)b$ är mindre än talet r. Detta är motstridigt, eftersom vi valde r att vara det minsta icke-negativa heltalet i mängden R. Därmed vet vi att $r < b$ och q och r är de eftersökta talen.

Om $b < 0$, ersätter vi talet b i förra beviset med det positiva talet $-b$. Då får vi istället talen q och r som uppfyller ekvationen $a = q(-b) + r = (-q)b + r$, där $r < -b = |b|$. Därmed är talen $-q$ och r de tal som är efftersökta.

Vi fortsätter med att bevisa att de funna talen är entydiga. Låt oss anta att även talen q' och r' uppfyller satsens krav. Då får vi följande ekvation $qb + r = q'b + r'$. Från denna ekvation följer följande.

$$r - r' = (q' - q)b.$$

Såväl r som r' är icke-negativa tal, som är mindre än $|b|$. Vi kan därmed dra slutsatsen att $0 \leq |q - q'||b| = |r - r'| < |b|$, vilket i sin tur betyder att $0 \leq |q - q'| < 1$. Eftersom $|q - q'|$ är ett heltal så måste det följa att $|q - q'| = 0$. Därmed är $q = q'$ och $r = r'$. □

Resttermerna och deras användning kommer att tas upp mera när vi kommer till moduloräkning. Men för att underlätta en del bevis i framtiden, kommer jag ännu att ta i användning Lemma 4.3, samt bevisa det.

Lemma 4.3. *Talen a och b har samma rest när de delas med n, om och endast om $n|(a - b)$.*

Bevis. Vi börjar med att anta att a och b har samma rest r. Härmed $a = k_1 n + r$ och $b = k_2 n + r$ för några $k_1, k_2 \in \mathbb{Z}$. Nu är $a - b = (k_1 - k_2)n$ delbart med talet n.

Vi antar att $n|(a-b)$, vilket betyder $a-b = kn$ för något $k \in \mathbb{Z}$ och att sedan $a = b+kn$. Vi låter r vara resttermen när b delas med n. Detta ger oss $b = qn + r$, där $q \in \mathbb{Z}$ och $0 \leq r \leq n$. Nu så är

$$a = b + kn = qn + r + kn = (q + k)n + r,$$

vilket ger att r också är resttermen för a. □

4.1.1 Största gemensamma delare

Heltal kan ha flera olika delare och olika heltal kan också ha samma delare. Talen n och m kan ha många gemensamma delare, men vi kommer fokusera på den största gemensamma delaren. Största gemensamma delare tas inte upp i mitt e-läromaterial, men kommer att behövas för att förklara vissa fenomen inom modulär aritmetik i ett senare skede. Vi måste därför definiera vad den största gemensamma delaren är.

Definition 4.4. Låt a och b vara positiva heltal. Den största gemensamma delaren (sgd) till talen a och b är det största positiva heltalet $d \in \mathbb{Z}$ som delar både a och b.

4.2 Primtal och primtalsfaktorisering

Primtal är ett viktigt begrepp inom den del av kryptografin som jag behandlar i mitt e-läromaterial. Vi börjar med att definiera vad ett primtal är.

Definition 4.5. Ett heltal $p > 1$ är ett primtal, om det endast är delbart med sig självt och 1.

De första primtalen är $2, 3, 5, 7, 11 \ldots$ Hittills har man inte hittat någon algoritm som enkelt kan finna stora primtal, men det man dock vet är att det finns oändligt av dem, vilket vi också snart kommer att bevisa. Förutom att primtal är viktiga inom RSA-kryptering så är primtalen en viktigt del av alla heltals uppbyggnad. Detta eftersom alla tal kan skrivas som en produkt av primtal. Förutom det att alla tal går att skriva som en produkt av primtal, så är kombinationen av dessa tal entydiga. Detta betyder med andra ord att primtalsfaktoriseringen är entydig.

Definition 4.6. Ett tal p kallas för en primtalsfaktor till talet n om p är ett primtal och $p \mid n$.

Som exempel är primtalsfaktorerna till talet 30 talen $2, 3$ och 5, eftersom talet 30 är delbart med de nämnda talen och de alla är primtal.

Sats 4.7. *Alla positiva heltal kan skrivas som en produkt av primtal. Primtalsfaktorerna för varje positivt heltal är unika.*

Bevis. Vi börjar med att bevisa att varje positivt heltal går att skriva som en produkt av primtal. Låt $n > 1$ vara ett heltal. Om n är ett primtal så är vi klara, eftersom primtal endast är delbart med sig själv och talet 1. Om n inte är ett primtal kan man skriva $n = n_1 n_2$, där $1 < n_1 < n$ och $1 < n_2 < n$. Om n_1 och n_2 är primtal så är vi klara. Om så inte är fallet kan ett av talen, eller bådadera skrivas som en produkt av två tal. Om vi fortsätter i samma mönster så kan n alltid skrivas som en produkt av mindre och mindre positiva heltal. Eftersom det här inte kan fortsätta för evigt kommer vi förr eller senare att nå en punkt där vi får primtalen $p_1, p_2, \ldots, p_r$ för vilka gäller att $n = p_1 p_2 \ldots p_r$.

Nu när vi visat att alla positiva heltal kan skrivas som en produkt av primtal, ska vi visa att kombinationen av primtal för varje heltal är entydigt. Vi antar att talet n går att skriva som en produkt av primtal i två olika former.

$$n = p_1 p_2 \ldots p_r \;\; \textit{och} \;\; n = q_1 q_2 \ldots q_s.$$

Eftersom p_1 delar talet n så delar p_1 också något av talen q_i. Detta bygger på det faktum att om ett primtal delar produkten $a_1 a_2 \ldots a_t$, så delar p något av talen a_j. Vi antar nu att $q_i = q_1$. Eftersom både p_1 och q_1 är primtal är enda möjligheten den att $p_1 = q_1$. Detta ger oss nu att

$$p_2 p_3 \ldots p_r = q_2 q_3 \ldots q_s.$$

Om vi fortsätter på samma sätt så kommer vi fram till att $p_i = q_i$ för alla i och att därav följer att $r = s$. Detta betyder att de båda formerna av produkten är samma. □

Sats 4.8. *Det finns oändligt många primtal.*

Bevis. Anta att satsen är osann och att det bara finns ett ändligt antal primtal. Låt de vara $q_1, q_2, \ldots, q_n$. Vi betraktar talet $m = q_1 q_2 \ldots q_n + 1$. Vi vet att $m > q_1, q_2, \ldots, q_n$ och därmed är $m \neq q_1, q_2, \ldots, q_n$ vilket betyder att m inte är ett primtal.

Eftersom Sats 4.7 säger att alla tal kan skrivas som en entydig produkt av primtal måste det existera ett q_k som är en delare till m. Då gäller

$$q_k \mid m \;\; och \;\; q_k \mid q_1 q_2 \ldots q_n.$$

Enligt Lemma 4.3 har m och $q_1 q_2 \ldots q_n$ samma rest vid division med q_n om och endast om

$$q_k \mid (m - q_1 q_2 \ldots q_n).$$

Eftersom $m - q_1 q_2 \ldots q_n = 1$, betyder det att $q_k \mid 1$. Detta stämmer inte, vilket betyder att det måste finnas oändligt med primtal. □

4.2.1 Eratosthenes såll

Som tidigare nämnt är det mycket arbetsamt att hitta stora primtal, eftersom det inte finns någon enkel algoritm för det. För att undersöka om ett tal n är ett primtal kan man som alternativ undersöka om något $1 < d < \sqrt{n}$ är en delare till n. En annan metod som nämns i e-läromaterialet är Eratosthenes såll. Eftersom denna metod nämns specifikt har jag tänkt gå genom hur metoden går till.

1. Vi börjar med att skriva en tabell med alla tal $\{2, 3, \ldots n\}$.
2. Vi undersöker nu talet 2. Eftersom 2 är ett primtal får den stå kvar i vår tabell. Alla tal delbara med 2 stryks dock över, eftersom de inte är primtal.
3. Nästa tal i tabellen är 3. Detta tal är igen ett primtal och får stå kvar i tabellen. Igen så stryks alla tal som är delbara med 3 bort från tabellen.
4. 5 kommer att vara nästa tal i tabellen som inte är överstrykt. 5 är därmed ett primtal och får stå kvar, medan alla tal delbara med 5 stryks bort.
5. Vi forsätter på följande vis till vi nått talet $\sqrt{n}$. Detta eftersom varje tal mindre än n som inte är ett primtal måste vara delbart med $k \leq \sqrt{n}$, där $k \in \mathbb{N}$. Orsaken till detta är att om endast $k > \sqrt{n}$ och $l > \sqrt{n}$ delar n, så $kl > (\sqrt{n})^2 = n$. Däremed innehåller tabellen endast primtal när vi nått $\sqrt{n}$.

4.3 Kongruensaritmetik

Kongruensaritmetik, eller modulär aritemtik som man också kan kalla det, är en av stöttestenarna för RSA-kryptering. Det var alltså väsentligt för mitt e-läromaterial att ta

med ett kapitel om det. Användningen av kongruensräkning är mycket enkel och kan därför anpassas till högstadieundervisning, men för att verkligen förstå vad uträknignarna innebär krävs mer än vad e-lärmaterialet erbjuder. För att börja nysta upp kongruensaritmetik som koncept, börjar vi med att definiera vad kongruens mellan tal betyder.

Definition 4.9. Låt talen $a, b \in \mathbb{Z}$ och $n \in \mathbb{N}$ givet. Talen a och b är kongruenta modulo n om $n \mid (a - b)$. Detta betecknar vi $a \equiv b (\text{mod } n)$.

Det här betyder att $a - b = kn$ för något $k \in \mathbb{Z}$. Tanken är alltså att alla de tal vilka får samma rest r när de divideras med m är kongruenta med varandra. Om $n \nmid (a - b)$ skriver vi istället $a \not\equiv b (\text{mod } n)$. Till exempel så $5 \equiv 15 (\text{mod } 10)$, men $12 \not\equiv 13 (\text{ mod } 27)$.

Sats 4.10. *Låt $a, b, c, d \in \mathbb{Z}$ och låt också n vara ett positivt heltal. Då gäller följande påståenden. Om*

$$a \equiv b (mod\ n) \ \ och \ \ c \equiv d (mod\ n)$$

så

$$a + c \equiv b + d (mod\ n) \ \ och \ \ ac \equiv bd (mod\ n)$$

Bevis. Vi börjar med att anta att $a \equiv b (\text{mod } n)$ och $c \equiv d (\text{mod } n)$. Det här betyder att det existerar sådana $k, l \in \mathbb{Z}$ så att följande ekvationer gäller: $a = b + kn$ och $c = d + ln$. Det vi då märker är:

$$a + c = b + kn + d + ln = (b + d) + (k + l)n,$$

vilket i sin tur betyder att $a + c \equiv b + d (\text{mod } n)$. Vi fortsätter med att undersöka påståendet $ac \equiv bd (\text{mod } n)$. Vi har samma antaganden som i ovanstående bevis, från vilka vi kan göra samma slutsatser gällande $a = b + kn$ och $c = d + ln$. Den här gången märker vi att:

$$ac = (b + kn)(d + ln) = bd + bln + knd + knln$$

$$= bd + (bl + kd + kl)n,$$

vilket i sin tur bevisar att $a + c \equiv b + d (\text{mod } n)$. □

Utifrån den ovanstående satsen kan vi också enkelt bevisa följande sats.

Sats 4.11. *Låt $a, b \in \mathbb{Z}$. Om $a \equiv b (mod\ n)$, så gäller också $a^m \equiv b^m (mod\ n)$ för alla icke-negativa heltal m.*

Bevis. Låt $a, b \in \mathbb{Z}$ och anta att $a \equiv b \pmod{n}$ gäller. Vi använder induktion för att visa att $a^m \equiv b^m \pmod{n}$ för alla $m \in \mathbb{N}$.

1. Vi visar att påståendet gäller för $m = 2$. Eftersom $a \equiv b \pmod{n}$ så säger sats 4.10 att $aa \equiv bb \pmod{n}$. Därmed gäller även $a^2 \equiv b^2 \pmod{n}$.

2. Vi antar att påståendet gäller för $m = k$, alltså att $a^k \equiv b^k \pmod{n}$ för $k \in \mathbb{N}$.

3. Vi visar att påståendet gäller för $m = k + 1$. Eftersom $a \equiv b \pmod{n}$ och $a^k \equiv b^k \pmod{n}$ så säger sats 4.10 att

$$aa^k \equiv bb^k \pmod{n},$$

alltså gäller

$$a^{k+1} \equiv b^{k+1} \pmod{n}.$$

Induktion på k ger $a^m \equiv b^m \pmod{n}$ för alla $m \in \mathbb{N}$

□

Fermats lilla sats och Eulers φ-sats

Beräkningar av kongruenser är något invecklat, men de blir betydligt lättare med hjälp av Fermats lilla sats och Eulers φ-sats. Eulers φ-sats fungerar mest som en generalisering av Fermats lilla sats och bådadera bevisas på samma sätt.

Sats 4.12. *Låt p vara ett primtal och a vara ett heltal. Låt också $sgd(a, p) = 1$. Då gäller att*

$$a^{p-1} \equiv 1 (mod\ p).$$

Bevis. Låt $S = \{1, 2, 3, \ldots, p-1\}$. Vi påstår nu att mängden $a \cdot S (\text{mod } p)$, vilken innehåller produkten av elementen ur S med a beräknade från modulo p endast är en permutation av S. Med andra ord

$$S = \{1a, 2a, \ldots, (p-1)a\} \pmod{p}.$$

Härmed är inga ia för något $1 \leq i \leq (p-1)$ delbara med p, eftersom om $p \mid ja$ så $p \mid j$ eller $p \mid a$, vilket inte är möjligt. Därmed räcker det att bevisa att alla element i $a \cdot S \pmod{p}$ är distinkta. Vi antar att $ai \equiv aj \pmod{p}$. Eftersom $sgd(a, p) = 1$ så betyder det att $i \equiv j \pmod{p}$, vilket betyder att $i = j$ då $1 \leq i, j \leq (p-1)$.

Detta ger oss alltså att produkten av elementen i S är

$$2 \cdot 3 \cdot \ldots \cdot (p-1)a^{p-1} \equiv 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p}.$$

Vi kan utesluta faktorerna $1, 2, \ldots, p-1$ från båda sidorna, eftersom $p \nmid j$ då $j = 2, 3, \ldots, (p-1)$. Då vi gör det så blir endast följande uttryck kvar $a^{p-1} \equiv 1 (mod\ p)$. □

Definition 4.13. Två tal m, och n är relativt prima om $sgd(m, n) = 1$.

För att kunna förstå Eulers sats måste vi börja med att definiera Eulers φ-funktion. Om funktionen appliceras på ett positivt heltal n så ger den oss antalet positiva heltal mindre än eller lika med n som är relativt prima med n:

$$\varphi(n) = |\{1 \leq m \leq n : sgd(n, m) = 1\}|.$$

Till exempel är $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$ o.s.v. Som specialfall kan vi notera att $\varphi(p) = p - 1$ då p är ett primtal.

För att härleda formeln börjar vi med att definiera primtalsfaktoriseringen av n som följande: $n = \prod_{i=1}^{m} p_i^{e_i} = p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}$ där p_i är distinkta primtal. Vi kan nu använda oss av principen om inklusion/exklusion som argument för att beräkna antalet siffror som är mindre än eller lika med och relativt prima till n. Två heltal är relativt prima om och endast om deras största gemensamma nämnare är 1. Vi börjar med att beräkna komplementet till det vi vill ha. Det finns $\frac{n}{p_1}$ positiva heltal som är mindre än, eller lika med n och vilka är delbara med p_1. Om vi gör samma sak för alla p_i och adderar dessa, får vi följande summa:

$$\frac{n}{p_1} + \frac{n}{p_2} + \ldots + \frac{n}{p_m} = \sum_{i=1}^{m} \frac{n}{p_i}.$$

Eftersom vi för tillfället har för stort antal siffror fortsätter vi med att reducera antalet genom att subtrahera bort de tal som är delbara med två olika p_i. Antalet sådana siffror är:

$$\sum_{1 \le i_1 < i_2 \le m} \frac{n}{p_{i_1} p_{i_2}}.$$

Vi använder oss av principen om inklusion/exklusion för att motivera att siffrorna i komplementet till vad vi vill ha är

$$\sum_{1 \le i_1 \le m} \frac{n}{p_i} - \sum_{1 \le i_1 < i_2 \le m} \frac{n}{p_{i_1} p_{i_2}} + \ldots + (-1)^{m-1} \frac{n}{p_{i_1} p_{i_2} \dots p_m}.$$

Summan representerar antalet siffror mindre än n som delar en gemensam faktor med n, så

$$\varphi(n) = n - \left(\sum_{1 \le i_1 \le m} \frac{n}{p_i} - \sum_{1 \le i_1 < i_2 \le m} \frac{n}{p_{i_1} p_{i_2}} + \ldots + (-1)^{m-1} \frac{n}{p_{i_1} p_{i_2} \dots p_m} \right)$$

$$= n \left(1 - \sum_{1 \le i_1 \le m} \frac{1}{p_i} + \sum_{1 \le i_1 < i_2 \le m} \frac{1}{p_{i_1} p_{i_2}} - \ldots + (-1)^{m} \frac{1}{p_{i_1} p_{i_2} \dots p_m} \right)$$

$$= n \left(1 - \frac{1}{p_1} \right) \left(1 - \frac{1}{p_2} \right) \dots \left(1 - \frac{1}{p_m} \right).$$

Givet primtalsfaktoriseringen $n = p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}$ kan vi nu alltså beräkna $\varphi(n)$ genom att använda följande formel:

$$\varphi(n) = n \left(1 - \frac{1}{p_1} \right) \left(1 - \frac{1}{p_2} \right) \dots \left(1 - \frac{1}{p_m} \right).$$

Nu när vi härlett Eulers φ-funktion kan vi gå vidare till Eulers φ-sats.

Sats 4.14. *Låt a och n vara positiva heltal. Låt också $sgd(a, n) = 1$. Då gäller att*

$$a^{\varphi(n)} \equiv 1(mod\ n).$$

Bevis. Satsen bevisas på samma sätt som sats 4.12, där vi i detta fall låter
$S = \{1 \leq m \leq n : sgd(n, m) = 1\}$. □

4.4 RSA-kryptering

RSA-systemet är en krypteringsmetod som skapades 1977 av Ron Rivest, Adi Shamir, and Leonard Adleman, vilkas initialer fick ge namnet till krypteringsmetoden. I dagens läge är RSA-krypteringen en mycket vanlig krypteringsmetod, eftersom den anses vara väldigt säker. RSA-kryptering är dock en ganska långsam krypteringsmetod och den används därför sällan för att kryptera användardata, utan används mest för att säkert skicka krypterade nycklar. RSA-kryptering har sin grund i elementär modulär aritmetik och bygger på det faktum att det är svårt och långsamt att hitta faktorer till mycket stora tal.

Varje användare A i systemet väljer två stycken primtal p och q, där $p \neq q$. Ju större primtal desto säkrare blir krypteringen. I vanliga fall används cirka 100-siffriga primtal, eftersom de anses vara tillräckligt säkra. Med dessa primtal gör man två olika beräkningar. Först beräknar man den offentliga nyckeln n, vilken alltså är offentlig för allmänheten. Sedan beräknar man $\varphi(n)$ (Eulers funktion), vilken kommer hjälpa oss att välja tal i ett senare skede.

$$n = pq \quad och \quad \varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1).$$

Användare A väljer också två tal till, e och d. För dessa tal bör det gälla att $1 < e, d < \varphi(n)$ och $ed \equiv 1(\text{mod } \varphi(n))$. När man väljer ett e så bör man välja ett sådant e som är relativt primt till $\varphi(n)$ och därefter beräkna dess modulära multiplikativa invers $e^{-1} \equiv d(\text{mod } \varphi(n))$. Därefter är det enkelt att beräkna d genom att lösa diofantiska ekvationen $ed - x\varphi(n) = 1$ (x och d okända), eftersom man då vet såväl e som $\varphi(n)$. Talet e kommer vara en del av den offentliga nyckeln till allmänheten, medan d kommer vara en del av den hemliga nyckeln, som endast delas med de som ska dekryptera meddelandet. Den offentliga nyckeln består nu av (n, e) och d är den hemliga nyckeln. För att man forsättningsvist ska kunna hålla d hemligt bör också p, q och $\varphi(n)$ hållas hemliga, eftersom man med dessa enkelt beäknar d då man vet den offentliga nyckeln. Den hemliga nyckeln består alltså av $(p, q, d, \varphi(n)$.

Krypterings- och dekrypteringsfunktionerna för användare A ser ut enligt följande. För att kryptera talet $1 \leq \omega \leq n$ används följande formel:

$$\omega' \equiv \omega^e(mod\ n).$$

För att i sin tur dekryptera talet ω används följande formel:

$$\omega'' \equiv \omega'^d(mod\ n).$$

Nedan visar vi att funktionerna är inversa permutationer av varandra, med andra ord att det krypterade meddelandet verkligen kan dekrypteras med den givna funktionen.

Sats 4.15. *Givet att* $\omega' \equiv \omega^e (mod\ n)$ *och* $\omega'' \equiv \omega'^d (mod\ n)$*, så* $\omega \equiv \omega'' (mod\ n)$ *för alla* $\omega \in \mathbb{N}$.

Bevis. Från de två funktionerna kan vi enkelt härleda följande.

$$\omega'' \equiv \omega'^d \equiv \omega^{ed} (mod\ n).$$

Enligt Eulers sats så vet vi följande

$$\omega^{\varphi(n)} \equiv 1 (mod\ n).$$

Eftersom $ed = 1 + k(p-1)(q-1)$ för något heltal k, så får vi följande påstående

$$\omega^{ed} = \omega^{1+k\varphi(n)} (mod\ n),$$

om $sgd(\omega, n) = 1$

□

RSA-kryptering har dock en viss svaghet. Denna svaghet ligger i att $p - q$ inte får vara för litet. Om $p - q$ är för litet går det lätt att hitta faktorerna p och q till $n = pq$ och RSA-krypteringen går att lösa.

Sats 4.16. *Om* $| \frac{p-q}{2} |^2 < 2\sqrt{n} + 1$ *så är det lätt att hitta faktorer till talet* $n = pq$.

Bevis. Vi börjar med att anta att $p = q$. Om detta är fallet går det lätt att hitta faktorer eftersom $p = \sqrt{n}$. Om vi istället antar att $p > q$ och betecknar $p = t + r$ och $q = t - r$, där t och r är positiva heltal. Det betyder att $p - q = t + r - t + r = 2r$. Det här betyder alltså,

$$| \frac{p-q}{2} |^2 = | \frac{2r}{2} |^2 = r^2.$$

Vilket i sin tur betyder att $r^2 < 2\sqrt{n} + 1$. Vi vet också följande,

$$n = pq = (t + r)(t - r) = t^2 - r^2.$$

Vi fortsätter med att undersöka $(\lceil \sqrt{n} \rceil + 1)^2$.

$$\left(\lceil \sqrt{n} \rceil + 1\right)^2 = \lceil \sqrt{n} \rceil^2 + 2\lceil \sqrt{n} \rceil + 1 > n + 2\sqrt{n} > n + r^2$$

Vi kan från tidigare kunskap härleda att $t^2 = n + r^2$. Detta betyder i sin tur att $t^2 > n$, men $t^2 < (\lceil \sqrt{n} \rceil + 1)^2$ enligt det vi just visat. Detta betyder alltså att $t = \lceil \sqrt{n} \rceil$. Härmed kan vi använda t för att lösa ut r.

$$r^2 = \lceil \sqrt{n} \rceil^2 - n$$

Eftersom vi nu vet både r och t kan vi lösa ut p och q och därmed bryta RSA.

$$p = \lceil \sqrt{n} \rceil + r$$

$$q = \lceil \sqrt{n} \rceil - r.$$

□

RSA-kryptering är alltså väldigt säkert så länge vi väljer rätt sorts p och q. Med detta bevis så kommer jag att avsluta delen om RS-krypteringA och även min pro gradu avhandling.

Målet med min pro gradu avhandling ha varit att skapa ett temabaserat e-läromaterial för niondeklassister. Detta har jag lyckats med, men trots detta finns det alltid möjlighet att i framtiden utveckla e-läromaterialet varefter användningen av det visar på brister eller andra utvecklingsmöjligheter. Precis som skolvärlden är i ständig förändring, strävar jag att även e-läromaterialet kommer att få utvecklas med tiden.

Litteraturförteckning

[1] Alvarez, D., Moreno, D., Orduna, P., Pascual, V. & san Vicente, F. (2015). *Maths: from distance to e-learning.* International Journal of Interactive Multimedia and Arti cial Intelligence, 3 (1), 5-12.

[2] Armstrong, T. (1998) *Barns olika intelligenser.* Jönköping: Brain Books.

[3] Barger, R. (1998) *Math for the Gifted Child.* Jeffersson City, MO: Gifted Association of Missouri.

[4] Bates, J. & Munday, S. (2005) *Able, Gifted and Talented.* Cornwall, Bodmin: MPG Books Ltd.

[5] Dean, J. (2006). *Meeting the learning needs of all children. Personalised learning in the primary school.* New York: Routledge.

[6] Eriksson, Y. (2010). *Elever med särskild matematisk begåvning - sex elevers tankar om sin grundskoletid* Examensarbete Högskolan i Gävle.

[7] Ernvall-Hytönen, A-M. (2013). *Elementär Talteori* Kursmaterial vid Helsingfors Universitet.

[8] Europarådet (1994) *Recommendation 1248 on education for gifted children.* Strasbourg: Council of Europe.

[9] Galbraith, P. & Haines, C. (1998). *Disentangling the Nexus: Attitudes to Mathematics and Technology in a Computer Learning Environment.* Educational Studies in Mathematics, 36 (3), 275-290.

[10] Gardner, H. (1999). *Intelligence Reframed: Multiple Intelligences for the 21st Century.* New York: Basic Books.

[11] Goodhew, G. 2009. *Meeting the needs of gifted and talented students.* London: Continuum International Publishing

[12] Häsä, J. & Rämö, J. (2012). *Johdatus Abstraktiin Algebraan* Helsingfors: Gaudeamus.

[13] Ilomaki, L. (2012) *Olika e-läromedel & Stöd expertmässigt arbete* Utbilningsstyrelsen: Med kvalitet i fokus - E-läromedlen i undervisning och lärande.

[14] Jaakkola, T., Nirhamo, L., Nurmi, S. & Lehtinen, E. (2012) *Olika lärobjekt i en flexibel helhet.* Utbilningsstyrelsen: Med kvalitet i fokus - E-läromedlen i undervisning och lärande.

[15] Jaakkola, T. (2012) *Låt eleverna konfronteras med fenomenens komplexitet.* Utbildningsstyrelsen: Med kvalitet i fokus - E-läromedlen i undervisning och lärande.

[16] Koblitz, N. (1994). *A course in number theory and cryptography.* Springer-Verlag, New York, second edition.

[17] Krutetskii, V. (1976). *The psychology of mathematical abilities in schoolchildren.* Chicago: University of Chicago Press.

[18] Lehtonen, H. (1994) *Lahjakas oppilas koulussa.* Tampereen yliopisto. Hämeenlinnan normaalikoulun julkaisuja nro 3.

[19] Marland, S. P. Jr. (1971). *Education of the gifted and the talented: Report to Congress of the United States by the commissioner of Education.* Washington, D.C.: U.S. Government Printing Office.

[20] Männistö, R. (2013). *Miten tukea matemaattisesti lahjakasta oppilasta?* Luma-Sanomat 14.1.2013.

[21] Olszewski-Kubilius, P. & Lee, S.-Y. (2004). *Gifted Adolescents Talent Development Through Distance Learning.* Journal for the Education of the Gifted, 28 (1), 7-35.

[22] Pendarvis, E.D., Howley, A.A. & Howley, C.B. (1990). *The abilities of gifted children.* Englewood Cliffs, N. J.: Prentice Hall.

[23] Persson, R. S. (1997). *Annorlunda land, särbegåvningens psykologi.* Stockholm: Almqvist & Wiksell.

[24] Pettersson, E. (2008). *Hur matematiska förmågor uttrycks och tas om hand i en pedagogisk praktik.* Licentiatuppsats Växjö Universitet.

[25] Ruokamo, H. 2000. *Matemaattinen lahjakkuus ja matemaattisten sanallisten ongelmanratkaisutaitojen kehittyminen teknologiaperustaisessa oppimisympäristössä.* Helsingin yliopiston opettajankoulutuslaitos

[26] Smith, J. B. (1996). *Does an Extra Year Make Any Difference? The Impact of Early Access to Algebra on Long-Term Gains in Mathematics Attainment.* Educational Evaluation and Policy Analysis, 18 (2), 141-153.

[27] Tapola, A. & Veermans, M. (2012). *Väck och stöd intresse och motivation.* Utbildningsstyrelsen: Med kvalitet i fokus - E-läromedlen i undervisning och lärande.

[28] Utbildningsstyrelsen. (2014). *Grunderna för läroplanen för den grundläggande utbildningen 2014.* Helsingfors: Utbildningsstyrelsen.

[29] Utbildningsstyrelsen. (2013). *Med kvalitet i fokus - E-läromedlen i undervisning och lärande* Helsingfors: Utbildningsstyrelsen.

[30] Viro, E. (2014). *Projektioppiminen perusopetuksen vuosiluokkien 7-9 matematiikan opetuksessa.* Diplomarbete, Tampereen teknillinen yliopisto.

[31] Wallace, P. (2009). *Distance Learning for Gifted Students: Outcomes for Elementary, Middle, and High School Aged Students.* Journal for the Education of the Gifted, 32 (3), 295-320.

[32] Yli-Sikkilä, M. (2014). *Soveltavaa laskemista ja ongelmanratkaisua: Matemaattisesti lahjakkaiden oppilaiden eriyttäminen matematiikan lisämateriaaleilla.* Pro gradu-arbete, pedagogik, Tampereen yliopisto.

Bilaga 1

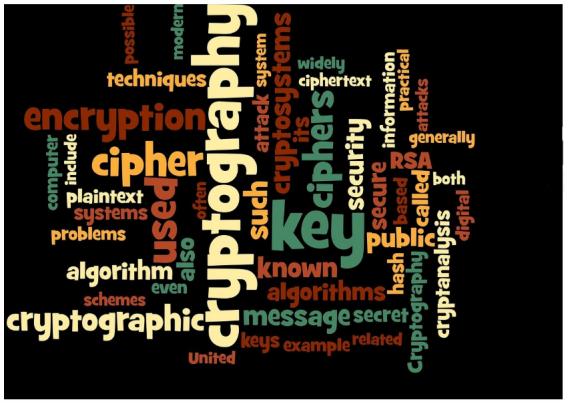
Överkursmaterial

Hem Kryptografi Caesarchiffer Primtal Moduloräkning RSA Källor

Kryptografi

Information om materialet

Detta material är skapat för en Pro-gradu avhandling. Den är dock öppen för allmänhetens bruk. Allt som finns här är bara att använda enligt eget tycke. Tag gärna kontakt om det finns några frågor gällande materialet, eller förbättringsförslag.



"Kryptografi" av tumbeldor Public Domain

Tanken bakom materialet

Materialet är specifikt planerat för niondeklassisters matematikundervisning. Tanken är att detta material kan användas som extra uppgifter när eleverna blir klara med givna uppgifter under lektionen. Materialet är helt temabaserat och i detta fall är temat kryptografi. Tanken är att eleverna själva ska jobba med materialet och lärarna mest ska fungera som handledare om behov för detta finns.

Hur använder jag hemsidan?

Hemsidan fungerar som ett temabaserat e-läromaterial för kryptografi. Varje flik, som man kan hitta uppe i högra hörnet, har ett eget tema med egna uppgifter och kan tänkas som kapitel i en bok. Jag föreslår att gå genom kapitlen i den ordning som de står, eftersom en del kunskap du får från tidigare kapitel behövs i kommande kapitel. Det är inte svårare än så, så välkommen att stiga in i kryptografins värld!

Bilaga 2

Överkursmaterial

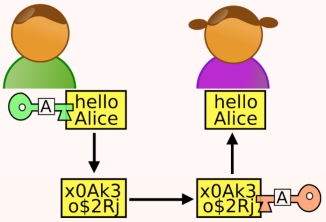
Hem Kryptografi Caesarchiffer Primtal Moduloräkning RSA Ta kontakt

Kryptografi

Vad är kryptografi?

Enligt it-ord.idg.se betyder ordet kryptografi *"konsten att hålla innehållet i meddelanden hemligt genom kryptering"*. Kryptering betyder i sin tur *"omvandling av ett meddelande i klartext till ett meddelande som är obegripligt för obehöriga"*.

Kryptering betyder med andra ord att man gör t.ex. en text obegriplig genom att ändra den enligt ett visst mönster. Detta mönster kan vara en krypteringsalgoritm eller t.ex. ett chiffer. Efter att man krypterat är texten sådan att ingen annan kan förstå den, förutsatt att de inte har en nyckel för hur de ska lösa krypteringen. En nyckel kan ses som ett system eller knep man ska följa för att dekryptera meddelanden. Dekryptering betyder att de kan omvandla meddelandet så att de får ut den ursprungliga texten.



"Asymmetric cryptography" av odder är licenserad under CC BY-SA 3.0

Ex.

> Stig-Helmer vill skicka det hemliga meddelandet *"Jag gillar dig"* till Ada. Han krypterar texten genom att ändra alla "g" till "w" och alla "a" till "ö". Den enkrypterade texten lyder enligt följande: *"Jöw willör diw"*. Han skickar meddelandet till Ada som har nyckeln för att dekryptera meddelandet. Nyckeln är i detta fall vilka bokstäver som ska ändras och till vad.

Historia

En av de tidiga krypteringarna som man känner till är Caesarchiffret, vilket vi kommer att prata mera om i ett senare kapitel. Denna form av kryptografi användes för första gången under Julius Ceasars livstid, ca 70 f.Kr.. Kryptering är alltså något som funnits väldigt länge och är inte någon ny uppfinning. Det har länge använts för att skicka hemliga meddelanden. I dagens läge är de meddelanden som skickas något annorlunda än tidigare.

Under andra världskriget använde tyskarna en kryptoapparat, kallad Enigma för att kryptera och dekryptera meddelanden. Tyskarna använde denna apparat före och under andra världskriget. En av anledningarna till att denna kryptoapparat blivit känd är det att de allierade lyckades dechiffrera många av de meddelanden som skickades via den. Det har gjorts en film under de senaste åren som återskapar händelserna kring dechiffreringen och filmen heter "*The Imitation Game*".

I dagens samhälle är inte kryptografi något ovanligt som endast används av spioner, eller hemlighetsmakare. Kryptografi är något som istället används nästan dagligen via till exempel din dator. När man loggar in på en hemsida med ett användarnamn och lösenord krypteras dessa så att ingen annan ska kunna fånga upp dem. När du surfar runt på internet kan du ibland märka att det står https:// istället för http:// på din webbadress, om det står https:// så surfar du runt på en enkrypterad sida. Detta betyder att informationen du delar där är krypterad och inte lika lätt att läsa för obehöriga. Detta är bara två vardagliga exempel på kryptering, men det finns oerhört mycket mer om man kollar noggrannare.

Kodspråk

Vad är kodspråk?

Exempel på kodspråk

Några av er har kanske hört talas om rövarspråket innan. Detta kodspråk kunde man läsa om i Astrid Lindgrens böcker om Kalle Blomkvist. I böckerna så använder Kalle Blomkvist språket för att kunna tala med sina vänner utan att någon annan förstod. Knepet för krypteringen är enkel. Låt oss säga att vi vill kryptera ordet potatis. För att göra detta, så sätter vi ett "o" efter varenda konsonant och sen repeterar vi samma konsonant en gång till. Vid vokaler så händer ingenting. Ordet potatis blir alltså popototatotisos.

Andra exempel.

> Raseborg ----------> Rorasosebobororgog
>
> Filosofiemagister ---------> Fofilolososofofiemomagogisostoteror
>
> Saxofon ----------> Sosakoksosofofonon (x skrivs som ks i rövarspråket)

Uppgifter

1. Det finns kodspråk som liknar rövarspråket, bl.a. *Pig Latin* och *fikonspråket*. Ta reda på hur de fungerar och försök hitta flera liknande kodspråk.
2. Skriv förklaringar till orden: kryptering, dekryptering, kryptografi, kryptologi, och kryptotext. Orden kan bl.a. hittas från https://it-ord.idg.se/
3. Hitta en artikel skriven om kryptografi och skriv en kort sammanfattning om den.
4. Vid vilka andra tillfällen i vardagen än de som nämndes i texten behövs kryptering?
5. Undersök hur Enigma-maskinen fungerar. Om du vill försöka skapa en egen Enigma-maskin finns information om det i följande länk: https://blogs.helsinki.fi/summamutikka/tag/enigma/

Bilaga 3

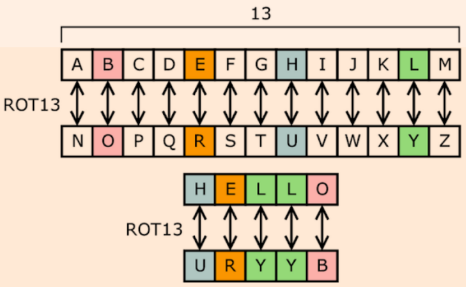
Caesarchiffer

Vad är ett chiffer?

Chiffer är det andra kodsystemet man kan använda sig av när man krypterar. Ett chiffer använder en serie uträkningar för att ändra bitar av t.ex. text till något annat. Chiffer är det vanligaste systemet för kryptering i dagens läge. Chiffer är svårare att dekryptera än kodsystemet och gör det därmed säkrare. Exempel på klassiska chiffer är Murarchiffret och Vigenère-chiffret.

Teori

I Caesarchiffret ersätter vi bokstäver med andra genom att rotera alfabetet framåt ett visst antal steg. Om vi har bokstaven A och roterar alfabetet framåt fyra steg får vi B, C, D, **E**. Bokstaven E ersätter därmed bokstaven A. När vi roterat så långt att vi nått fram till bokstaven Ö så fortsätter vi från bokstaven A, alltså början av alfabetet. Det finns några olika sätt att visualisera bokstavsbytet.



"ROT13" av Matt Crypto Public Domain

Alternativ 1

Man ritar upp en tabell med två rader som på bilden här bredvid. I den övre tabellen skriver man in bokstäverna i tur och ordning. I den nedre tabellen skriver du de roterade bokstäverna. Efter detta är det lätt att kryptera och dekryptera orden.

Alternativ 2

Rita igen upp en tabell med två rader enligt bilden nedan. Varje bokstav från en siffra som den representerar. Om man nu vill rotera åtta steg så adderar man bokstavens siffra med åtta. Bokstaven A skulle alltså med rotationen åtta bli I eftersom 1 + 8 = 9 och nian representeras i detta fall av I. Eftersom vi endast har 29 bokstäver i alfabetet blir talet 30 samma som 1. Om vi får ett tal *n* större än 29 så kan vi räkna ut vilken bokstav det är fråga om genom att räkna *n* - 29.

A	B	C	D	E	F	G	H	I	...	T	U	V	W	X	Y	Z	Å	Ä	Ö
1	2	3	4	5	6	7	8	9	...	20	21	22	23	24	25	26	27	28	29

Uppgifter

1. Caesar skickar ett hemligt meddelande åt sina soldater. I egenskap av kryptograf får du i uppgift att kryptera hans meddelande. Meddelandet lyder enligt följande: "*Klockan fem, anfall gallerna.*" Caesar vill ha en rotation på 16 steg. Hur lyder den krypterade texten?

2. Dekryptera följande krypteringar: (talet inom parentes är rotationstalet)
   - IFKTBM (1)
   - KHOOR (3)
   - FSÖMSS (20)

3. Hitta på två orsaker till att Caesarchiffret inte är särskilt säkert krypteringssystem.

4. Du får ett krypterat meddelande på Whatsapp av en okänd person, "*Ghwwd bu hww khpoljw phgghodqgh*". Du är bekant med Ceasarchiffret från tidigare och inser att krypteringen bygger på det systemet. Försök dekryptera meddelandet utan att veta rotationen. Skriv ett svar tillbaka till avsändaren med samma rotationsantal.

Bilaga 4

Primtal och primtalsfaktorisering

Teori

Primtal

Primtal är positiva heltal större än 1 som endast kan uttryckas som en produkt av sig självt och talet ett. Man kan också tänka sig att ett primtal endast är delbart med sig själv och siffran 1.

Ex 1.

7 är ett primtal eftersom endast $7 \times 1 = 7$, det går alltså inte att multiplicera några andra heltal för att få produkten 7.

8 är däremot inte ett primtal, eftersom $8 \times 1 = 8$, men också $4 \times 2 = 8$. Det finns alltså olika multiplikationsvariationer för att få produkten 8.

-3 är inte heller ett primtal, eftersom primtal endast är positiva heltal.

Det finns oändligt med primtal. Primtalen följer inte heller något mönster (åtminstone inte ett mönster någon matematiker hittills har hittat), vilket kan göra det svårt för människor att hitta dem. Datorer kan dock hitta väldigt stora primtal och snabbt.

Primtalsfaktorisering

Primtalsfaktorisering innebär att man skriver ett tal som en produkt av primtal. Man faktoriserar med andra ord ett tal tills endast primtal står kvar som faktorer. Alla positiva heltal kan skrivas som en produkt av primtal.

Ex 2.

Vi primtalsfaktoriserar talet 432.

$432 = 216 \times 2$ Vi börjar med att faktorisera ut primtalet 2, eftersom 432 är ett jämnt tal.

$= 108 \times 2 \times 2$

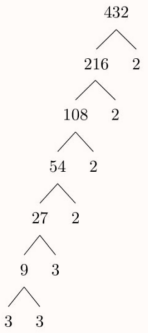
$= 54 \times 2 \times 2 \times 2$ Vi faktoriserar ut talet 2, tills det inte är möjligt mera.

$= 27 \times 2 \times 2 \times 2 \times 2$ Eftersom talet 27 är udda, försöker vi hitta ett annat primtal att faktorisera ut.

$= 9 \times 3 \times 2 \times 2 \times 2 \times 2$

$= 3 \times 3 \times 3 \times 2 \times 2 \times 2 \times 2$ När det endast finns primtal som faktorer är faktoriseringen klar.

Vi kan också ta hjälp av ett så kallat faktorträd. Faktorträdets grenar representerar de olika faktorerna. Nedan finns en bild som visar hur faktorträdet används.



Ändarna på grenarna visar vilka tal som är faktorer till 432. Teorin är den samma som när man vanligt faktoriserar, faktorträdet är mer ett sätt att förtydliga och åskådliggöra fenomenet.

Uppgifter

1. Vilka av talen -13, 5, 15, 97 och 103,3 är primtal? Motivera.

2. Räkna upp alla primtal mellan 1-100. Som tips till denna uppgift kan man söka upp Eratosthenes såll på nätet.

3. Primtalsfaktorisera talen 16, 124 och 325.

4. Om produkten av x och y är ett primtal, vad vet du om talen x och y?

Extra tankenöt

I en familj finns sex barn. Fem av barnen är 2, 6, 8, 12 respektive 14 år äldre än det yngsta barnet. Alla åldrarna i familjen är primtal. Hur gammalt är det yngsta barnet?

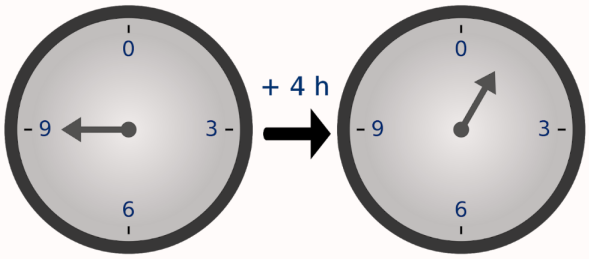
Bilaga 5

Moduloräkning

Teori

Klockaritmetik

När vi börjar med moduloräkning kan börja med att föreställa sig en klocka. Om man har en vanlig väggklocka hemma så ser man att den går från 1 till 12. Efter att klockan blivit 12 så går den tillbaka till 1. Om man däremot har en digital klockan så kommer klockan att gå till 13. I detta fall är alltså 13 och 1 samma sak. Detta är grunden till klockaritmetik, eller moduloräkning. Den analoga klockan rör sig i vad man kallar modulo 12, alltså innehåller den alla tal mellan 1 och 12, men innehåller inga andra tal, t.ex. 16 existerar inte i modulo 12. Den digitala klockan rör sig i modulo 24, eftersom vi efter 24 går tillbaka till 1.



"Clock group" av Spindled är licenserad under CC BY-SA 3.0

Ex.

> Vi antar att vi har en klocka som rör sig i modulo 15. Vi antar också att vi har en räkneoperation ◷ som adderar ihop två klockslag. Beräkna 9◷9◷9.
>
> Vår räkneoperation adderar ihop klockslag och därmed får vi följande uträkning 9 + 9 + 9 = 27.
>
> För att få reda på vad 27 är i vår 15 modulos klocka dividerar vi 27 med 15 och kontrollerar vad vår rest blir.
>
> 27/15 = 1 rest 12.
>
> Resten berättar åt oss vad klockan är, den är alltså 12.

Modulär aritmetik

Om vi vill skriva vårt tidigare exempel på ett mer officiellt sätt kan vi skriva det så här:

$$27 \equiv 12 \pmod{15}$$

I klar text står det att 27 och 12 är kongruenta i modulo 15. Detta betyder alltså att i modulo 15 är 12 och 27 samma tal. För att skriva upp liknande situationer kan vi använda följande modell:

$$a \equiv b \pmod{n}$$

För att beräkna modulär aritmetik kan vi så som i vårt exempel dividera och få ut resten, eller sen subtrahera a och b med vårt modulo n, tills vi kommer till ett tal mindre än vårt tal n. På detta sätt går vi också eventuellt genom andra kongruenta tal till a och b. Vi kan också subtrahera så långt att vi kommer till negativa tal. Negativa tal kan också vara kongruenta med a och b.

Uppgifter

1. Vi har en klocka som rör sig i modulo 14. Bestäm följande klockslag.
   - 5 ◷ 5
   - 8 ◷ 12
   - 12 ◷ 12 ◷ 12
   - 17 ◷ 5
2. Räkna upp 5 tal som är kongruenta med 3 (mod 8), varav två bör vara negativa.
3. Är följande påståenden sanna?
   - $17 \equiv 25 \pmod{5}$
   - $69 \equiv 25 \pmod{11}$
   - $31 \equiv 53 \pmod{7}$
4. Om vi vet följande: $x \equiv 0 \pmod{y}$. Vad säger detta oss om sambandet mellan x och y?

Bilaga 6

RSA

Fakta

RSA är en mycket vanlig krypteringsmetod. Den anses vara en av de säkrare metoderna och därför använder bl.a. Ålandsbanken denna metod för att kryptering vid inloggning till nätbanken. RSA är dock en ganska långsam krypteringsmetod och den används därför sällan för att kryptera användardata, utan används mest för att skicka krypterade nycklar säkert. Krypteringsmetoden fick sitt namn efter upphovsmännens initialer, Rivest, Shamir och Adleman. RSA grundar sig på att om vi har två väldigt stora primtal så är det enkelt att multiplicera dem, men om man inte vet något annat än produkten är det svårt att faktorisera talet.

Teori

Varje användare av systemet väljer själv två stycken primtal p och q. Ju större primtal desto säkrare blir krypteringen. I praktiken används ca 100-siffriga primtal för att göra krypteringen säker. Med våra primtal gör vi två nya beräkningar

$n = pq$ och $m = (p - 1)(q - 1)$

Ex.

Vi väljer $p = 3$ och $q = 5$. Med dessa tal gör vi våra beräkningar.

$n = 3 \times 5 = 15$ och $m = (3 - 1) \times (5 - 1) = 2 \times 4 = 8$.

Efter att vi gjort våra beräkningar väljer vi två tal till e och d. För dessa tal ska det gälla att $1 < e, d < m$ och $ed \equiv 1 \pmod{m}$.

Ex.

Vi fortsätter på vårt tidigare exempel. Vi väljer e och d så att kraven uppfylls. $e = 3$ och $d = 3$. I vanliga fall väljer man två olika tal, men eftersom vi valt så små primtal har vi inte den möjligheten nu.

$1 < e, d < m$ vilket ger oss $1 < 3, 3 < 8$ **krav 1 uppfyllt.**

$ed = 3 \times 3 = 9$ vilket ger oss $9 \equiv 1 \pmod{8}$ **krav 2 uppfyllt.**

I RSA har vi alltid två så kallade nycklar för att kunna dekryptera meddelandet. En offentlig nyckel och hemlig nyckel. Efter alla våra uträkningar så har vi variabler vi behöver för våra nycklar. Den hemliga nyckeln, som man kan lista ut från namnet, hålls hemlig för omvärlden består av (p, q, m, d). Den offentliga nyckeln, som vem som helst kan se består av (e, n).

Hittills har vi samlat ihop variabler vi behöver för kryptering och först nu kan vi börja kryptera. Ganska ofta vill man kryptera bokstäver, men för att kunna göra det måste man förvandla bokstaven till en siffra först, te.x genom att låta bokstaven representera en siffra så som i kapitlet med Caesarchiffret. Vi kommer inte gå genom varför krypterings och dekrypterings formlerna fungerar, utan endast kolla hur man använder dem. Vi börjar med att kryptera ett tal w som måste uppfylla kravet $1 \leq w \leq n$, vi kan alltså inte kryptera ett tal större än vårt beräknade n. Krypteringsalgoritmen är följande:

$x \equiv w^e \pmod{n}$, där x representerar den enkrypterade siffran w.

Ex.

Vi fortsätter igen med de exempel vi haft tidigare. Vi väljer ett w som uppfyller kravet, $w = 2$. Efter detta krypterar vi talet.

$x \equiv w^e \pmod{n}$

$x \equiv 2^3 \pmod{15}$

$x \equiv 8 \pmod{15}$, vi kan nu välja vilket x som helst som är kongruent med 8 (mod 15).

$x = 23$. 23 är nu det enkrypterade talet för w.

För att dekryptera meddelandet använder man en formel som ser ut så här:

$y \equiv x^d \pmod{n}$.

Ex.

Använder som vanligt samma tal som i tidigare exempel.

$y \equiv x^d \pmod{n}$

$y \equiv 23^3 \pmod{15}$

$y \equiv 12167 \pmod{15}$ vi dividerar 12167 med 15 och får resten 2.

$y \equiv 2 \pmod{15}$ eftersom att vi vet att $1 \leq w \leq n$ så vet vi att 2 är talet vi söker efter.

$y = 2 = w$.

Uppgifter

1. Försök hitta program eller hemsidor som använder sig av RSA kryptering.
2. Beräkna de hemliga och offentliga nycklarna när du har valt $p = 13$ och $q = 7$. Talen e och d får du välja själv.
3. Antag att du som deltagare i ett RSA-system har offentlig krypteringsnyckel $n = 35$ och $e = 7$.
   (a) Kryptera meddelandena 6, 10 och 17.
   (b) Dekryptera de chiffrerade meddelandena 3 och 8
4. Visa att om för ett RSA-system talet p är känt (utöver n och e), så kan talet d lätt beräknas.

Bilaga 7

Ta kontakt

Via att fylla i följande formulär kan du ge direkt feedback gällande hemsidan. Såväl ris som ros tas tacksamt emot.